ADDRESSING THE 'FAILURE' OF INFORMED CONSENT IN ONLINE DATA PROTECTION: LEARNING THE LESSONS FROM BEHAVIOUR-AWARE REGULATION

Shara Monteleone†

CONTENTS

ABSTRACT 70
I. INTRODUCTION AND BACKGROUND 71
II. PRIVACY NOTICES AND PRIVACY PARADOX 78
A. *Information obligations and informed consent* 78
1. *Role of privacy policies in users' data disclosure* ... 81
2. *Personal data disclosure: direct and indirect* 83
3. *Data disclosure between individual autonomy and legal constraints* 83
4. *Limitations of the current safeguards: the privacy paradox* 86
B. *Addressing the drawbacks: alternative mechanisms to traditional privacy policies* 90
1. *A legal-technical approach* 90
2. *An integrated behavioural economic approach* 95
IIII. INSIGHTS FROM BEHAVIOURAL ECONOMICS ON INFORMATION PROVISION 97
A. *Applying behavioural science to policy: an overview* ... 97
B. *Applying behavioural science to policy: challenges and opportunities* 99
C. *Applying behavioural science to policy: from information overload to smart disclosure in Consumer Protection and in Data Protection* 103
IV. TOWARDS REGULATED PRIVACY NUDGES? 109
A. *Visceral notices* 110

† Senior researcher at STeP (Security, Technology & e-Privacy Research Group), European Technology Law, University of Groningen, The Netherlands

1. *The BREVE experimental project: Behavioural Responses to Privacy Visceral Notices* 112

B. *Integrating behavioural insights into privacy policy making?* 113

1. *Future research* 117

V. CONCLUSIVE REMARKS 118

ABSTRACT

Information notice and data subject's consent are the current main legal safeguards of data protection and privacy rights: they reflect individuals' instances, such as self-determination and control over one's own private sphere, that have been acknowledged in many jurisdictions. However, the theoretic strength of these safeguards appears frustrated by current online practices that seem suggesting to give-up with their most common form of implementation: privacy notices and request for consent. These measures are proving to be unsuccessful in increasing users' awareness and in fostering a privacy protective-behaviour. As recent studies have shown, although people declare privacy concerns, their actual behaviour diverges from their statements (the "privacy paradox"), as they seem to increasingly disclose personal data and to not even read privacy notices available online; eventually, the current privacy notices are not effective in regulating user's data disclosure.

Behaviourally informed approaches to regulatory problems, already applied to different areas of information provision and public policy, helped to clarify the reasons of similar peoples' behaviour that cannot be reduced to a simplistic "users do not care about privacy." Highlighting the regulatory weakness of traditional information notices, applied behavioural science has also demonstrated to be particularly effective in improving users' decision-making and attaining concrete policy objectives if accompanied by ad hoc design interventions to display the relevant, salient information. As users do not read privacy policies or act in contradiction with them, other strategies might be more successful in promoting, "nudging," privacy-protective behaviour.

The use of innovative information notices, like salient alerts and nudges, seems to be a promising means of behavioural change also in the area of digital privacy, a possible new area of application of behavioural insights.

Building on recent studies in the field (conducted mainly in the U.S.), this paper considers new forms of privacy notices (like "visceral"

notices), as alternative or complement to current legal (technical) measures for data protection. For the informed consent approach (or "notice and choice" approach) to work, it needs to be improved with well-designed, transparent and regulated nudging system, capable to help citizens in their decision-making as regards their privacy.

Without disregarding the challenges and limitations of nudging strategies in public policy in general and in the privacy area in particular, and examining their legal grounds, the paper aims also to integrate that branch of legal-policy research that see "nudging" methods as an effective way to gently encourage safer behaviours in the citizens.

I. INTRODUCTION AND BACKGROUND

The emergence of new digital technologies and the growth of an information-based economy, made data protection policy a priority in the European Union ("EU"), as well as in other countries' agenda, in which the search for a balance between the safeguard of individual fundamental rights and other competing interests is deemed crucial for the same existence of a democratic society. Information Communication Technologies ("ICTs"), despite being a key enabler for economic development, may also represent a threat to fundamental rights, namely to privacy and data protection rights, as enshrined by the Charter of Fundamental Rights of the EU.[1]

Safeguarding these rights plays a central role in building trust in the online environment. As the European Commission pointed out, building this trust is essential to economic development,[2] and it is a key objective in the Digital Agenda for Europe ("DAE"), the EU flagship initiative on all ICT-related activities.[3] For these reasons, the current legal framework

1. *See* Charter of Fundamental Rights of the European Union 326/02, art. 7-8, 2012 O.J. (C 391) 2 (containing two separate articles for privacy and data protection rights).

2. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 1, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Proposal for GDPR*].

3. *See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*, at 13, COM (2010) 245 final (May 19, 2010). The DAE, which includes more than 100 distinct actions, has as one of its goals to reinforce trust and security online. Action 35, in particular, aims to provide guidance in implementation of new Telecoms framework with regard to the protection of individuals' privacy and personal data (namely, of the e-*privacy* Directive 2002/58/EC as modified by Directive 2009/136/EC). *See Action 35: Guidance on Implementation of Telecoms Rules and Privacy*, EUROPEAN COMMISSION (Oct. 25, 2010), *available at* https://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy (last visited Dec. 18, 2015). Action 35 has to be read in conjunction with Action 12 (Review of the European Data Protection Rules)

on privacy and data protection in Europe is under review;[4] Directive 95/46/EC is going to be replaced by the General Data Protection Regulation ("GDPR"), which aims "to build a stronger and more coherent data protection framework in the EU."[5]

One of the main safeguards of the EU legal framework that the Proposal for a GDPR seeks to reinforce is represented by the fair information principles;[6] the transparency principle and consequent information obligations for those who process personal data is now strengthened and codified in the Draft Regulation, as a reinforcement of individual rights protection and an instrument of user empowerment.[7]

In particular, "Article 11 introduces the obligation on controllers to provide *transparent and easily accessible and understandable*

---

aimed at reviewing the current Data Protection regulatory framework "to strengthen individual rights and tackle emerging challenges from globalisation and new technologies." EUROPEAN UNION: CYBER SECURITY STRATEGY AND PROGRAMS HANDBOOK: VOLUME 1 STRATEGIC INFORMATION AND REGULATIONS 64, 73 (2014).

4. The legal framework currently applicable in the field of privacy and data protection is represented mainly by the Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, integrated by the Directive 2002/58/EC *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (so called e-*Privacy* Directive, as modified by the Directive 2009/136/EC, the e-*cookies* Directive). *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC); Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC); Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC).

5. *Proposal for GDPR*, *supra* note 2, at 2. The regulation, will apply to public and private processing of personal data in most of the activities related to the former I pillar of EU (the community pillar, including single market, consumer protection, social policy, etc.). The European Commission has a parallel initiative for the data protection in the area of police and judicial cooperation in criminal matters. *See Commission Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, at 15, COM (2012) 10 final (Jan. 25, 2012). Despite the adoption of these two separate legal instruments for data protection in different areas, given that the Lisbon Treaty (2009) has abolished the Pillar structure, the EC is firmly striving to adopt a *comprehensive* approach on data protection. *See Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 409, COM (2010) 609 final (Apr. 11, 2010) [hereinafter *A Comprehensive Approach on Personal Data Protection*].

6. *See* Paul De Hert & Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/45/EC: A Sound System for the Protection of Individuals*, 28 COMPUTER L. & SECURITY REV. 130, 134 (2012).

7. *See Proposal for GDPR*, *supra* note 2, at 25 ("The principles of fair and transparent processing require that the data subject should be informed in particular of the existence of the processing operation and its purposes, how long the data will be likely stored, on the existence of the right of access, rectification or erasure and on the right to lodge a complaint.").

information."[8] This is particularly relevant in situations such as online advertising, where the proliferation of actors and the technological complexity of practices make it difficult for the data subject to know and understand if personal data relating to them are being collected, by whom and for what purpose.[9] "Article 14 further specifies the controller's *information obligations* towards the data subject."[10]

This means that according to the transparency principle of the European legislation, any data controller, including an Internet company or an Internet Service Provider, must specify the types of data collected and the purposes for which they may be used.

Data processing and data flow are thus allowed under a number of conditions, namely the requirement of obtaining data subject's *consent* that should be *free, specific and informed.*

Directly connected to the transparency principle and information obligations, the *informed* (and also *free and specific*) *consent* requirement represents a cornerstone of the EU data protection legislation: it grants the main legal ground for personal data processing (although other legal basis are contemplated)[11] and it has been strengthened by the Draft GDPR, becoming now an *explicit consent*[12] requirement.

---

8. *Id.* at 8.

9. *See id.* at 43 ("Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject."); *id.* at 47 ("1. The controller shall have t*ransparent and easily accessible policies* with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an *intelligible form*, using *clear and plain language*, adapted to the data subject, in particular for any information addressed specifically to a child.") (emphasis added); *see also id.* at 24 (urging, in particular for children, specific protection and a clear language).

10. *Proposal for GDPR*, *supra* note 2, at 8 (emphasis added).

11. *Id.* at 43-44.

> 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:
> (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract . . . .

Id.

12. *See id.* at 42 ("'[T]he data subject's consent' means any *freely given specific, informed and explicit* indication of his or her wishes by which the data subject, either by a statement or by a *clear affirmative action*, signifies agreement to personal data relating to them being processed.") (emphasis added). The need to examine ways to clarify and strengthen the consent requirement has been considered by the European Commission. *See A Comprehensive Approach on Personal Data Protection*, *supra* note 5, at 8-9.

> [I]n the online environment – given the opacity of privacy policies – it is often more difficult for individuals to be aware of their rights and give informed

It is understood that consent cannot be inferred implicitly, as inaction should not be perceived as the indication of users' wishes, and that it should be evidenced by *a statement or by a clear affirmative action*. This last aspect is particularly relevant for the online environment,[13] where user's inactivity cannot be considered as consent, but where a "click" might be accepted as valid consent (if all other conditions are met).[14]

This means that in the context of behavioural advertising (which is becoming the principal business model for companies in the digital economy), the informed *consent* requirement should be obtained, for instance, by the third-party advertisers tracking the users, before placing tracking *cookies* on a user's computer or before accessing information stored on the user's computer. For the consent to be *informed*, the user should be provided with information about, for instance, the sending and purposes of the cookies.[15]

The choice made by the European legislation is clearly for an *opt-in* system, where an active action to consent is required (as opposed to *opt-out* system where the consent is presumed by default, with the possibility for the user to change it).[16]

> consent. This is even more complicated by the fact that, in some cases, it is not even clear what would constitute freely given, specific and informed consent to data processing . . .

Id. at 9.

13. In this regard, it is important to notice that European Directive 2002/58/EC, the distinct directive for the protection of personal data in the electronic communications sector (i.e., the *e-Privacy* Directive) as amended by Directive 2009/136/EC, also requires companies to obtain the Internet users' consent, in particular before installing *cookies*, having the users been provided *with clear and comprehensive information*. *See* Council Directive 2002/58, art. 5, 2002 O.J. (L 201) 37 (EC). The relationship between the Draft General DP Regulation and the e-Privacy Directive still needs to be clarified, however the e-Privacy Directive does not seem affected by the reform (if not for technical adjustments) and it should work as *lex specialis* with respect to the General Regulation. *See Proposal for GDPR*, *supra* note 2, at 99.

14. *See* Council Directive 2002/58 2002 O.J. (L 201) 31 (EC) ("Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."); *see also Opinion of the Working Parking on the Protection of Individuals with Regard to the Processing of Personal Data on the "Definition of Consent,"* at 26 (July 13, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (last visited Dec. 18, 2015) [hereinafter *Opinion on the Definition of Consent*].

15. Council Directive 2009/136, 2009 O.J (L 337) 11 (EC). According to Recital 66 of Directive 2009/136/EC, modifying e-Privacy Directive "methods of providing information and offering the right to refuse should be as user-friendly as possible" and that, "[w]here it is technically possible and effective, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application." *Id.* (emphasis added); *see Opinion on the Definition of Consent*, *supra* note 14, at 32.

16. *See, e.g.*, *id.*

Now, it must be noticed that both the current Data Protection ("DP") Directives and the Draft Regulation, despite establishing those information obligations and consent requirements, contain few indications on *how* information should be provided to the user or how the latter could exercise her right to object to the processing of personal data. The common instruments usually adopted by data controllers to be compliant with the law are privacy policies (or notices).[17]

As studies conducted both in Europe[18] and outside Europe[19] have shown, the problem with current privacy polices is that they are not effective, at least not concerning the purpose of increasing users privacy awareness (risks and rights) nor of encouraging a more responsible data disclosure. These and similar studies,[20] in fact, have demonstrated that, although the majority of Internet users report to have concerns about privacy and to notice the presence of privacy notices or warning messages, most of them, especially young people, do not read these statements and keep disclosing personal data: this phenomenon is also called "privacy paradox."

Current privacy notices are ignored as they are often written in a not clear and easy language. In brief, they are hardly ever read by users and – even if read – very difficult to understand. The reality offers a scenario characterized by a lack of understanding by users of the ways personal data is collected, used and disclosed, as well as of potential risks with the consequence that the provision of users' consent is not really *informed.*

However, even when the level of clearness and completeness of privacy polices is satisfactory, i.e., when they fulfill the legal formal

17. Most common privacy notices attached to a webpage are usually accessible through a hyperlink and made of a long statement; they are supposed to explain what information is collected and for what purposes, how it is used and the choices offered to the users (e.g. how to update personal account or to modify the default settings). Some examples, taken from Ryanair and Google's websites, are provided here: *see, e.g.*, *Ryanair Website Privacy Statement*, RYANAIR, *available at* http://www.ryanair.com/ie/privacy-policy/ (last visited Dec. 18, 2015); *Privacy Policy*, GOOGLE, *available at* http://static.googleusercontent.com/media/www.google.com/it//intl/en-GB/policies/privacy/google_privacy_policy_en-GB.pdf (last visited Dec. 18, 2015).

18. *See, e.g.*, *Pan-European Survey of Practices, Attitudes & Policy Preferences as Regard Personal Identity Data Management*, JOINT RES. CTR. (2012), *available at* http://is.jrc.ec.europa.eu/pages/TFS/documents/EIDSURVEY_Web_001.pdf (last visited Dec. 18, 2015) [hereinafter *Pan-European Survey of Practices*].

19. *See, e.g.*, Janice Tsai et al., *What's it to you? A Survey of Online Privacy Concerns and Risks* (NET Institute, Working Paper No. 06-29, 2006); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J. L. & POL'Y FOR THE INFO. SOC'Y 543 (2008).

20. Mary Madden et al., *Teen, Social Media and Privacy Report*, PEW RES. CTR. (May 21, 2013), *available at* http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/ (last visited Dec. 18, 2015).

requirements, they fail to realize the main purpose of the law (at least of the European law), that is, to foster attentive users' decision-making and eventually a conscious data-disclosure behaviour.

As users do not read privacy policies or act in contradiction with them, other strategies might be more successful in obtaining privacy-protective behaviour. It is not enough that privacy policies are provided in a place easy to find on a website, but they also should have an impact on users' behaviour.

Providing simplified, standardized privacy information, although of some benefits, has proved to be also insufficient. Insights from behavioural economics have helped to understand why (as discussed in the next sections).

Finally, current privacy policies do not help users in making the best choices as regards to consent (or not) to data processing. They fail to realize one of the objectives of DP law, i.e., to ensure that people make pondered decisions about their data, and, as ultimate goal, to increase trust in online services. Therefore, there may be a need of policy intervention aimed at changing users' behaviour, introducing alternative, more effective ways of presenting information.

Knowing how users really behave with regard to their personal data (often in contrast with their statements) may play a relevant role in addressing the current "privacy paradox," as well as the gap between existing legal privacy safeguards and implementing tools.

Behavioural research has not only shown that there is a significant relationship between the content of privacy policies and individuals' privacy concerns/trust,[21] but also that an overload of information (e.g., long and complex texts) is counterproductive also in the privacy field.[22] Given that people are influenced by how information (on products, services, etc.) is presented, identifying the appropriate notice content and design to display online privacy information should also improve users' decision-making in this regard, helping them in attaining a greater empowerment online.[23] By making easier, agile and thus more effective the display of privacy information, in fact, users may be able to take more

21. Kuang-Wen Wu et al., *The Effect of Online Privacy Policy on Consumer Privacy Concern and Trust*, 28 COMPUTERS IN HUM. BEH. 889 (2012).

22. *See, e.g.*, Janice Tsai et al., *The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study*, 22 INFO. SYSTEM RES. 254 (2011); Alessandro Acquisti & Jens Grossklags, *What Can Behaviorual Economics Teach Us About Privacy*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES 363 (Alessandro Acquisti et al. eds., 2007).

23. *See generally* Sebastian Deterding et al., *Designing Gamification: Creating Gameful and Playful Experiences*, *in* CHI '13 CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 3263 (2013).

informed decisions regarding the usage of their personal information online.[24]

Experiments to test users' responses (their actual behaviour) to new type of privacy policies started to be run mainly in the U.S.,[25] while in Europe this aspect is still not enough explored. This paper gives briefly an account of the existing behavioural studies and experiments, including, though, the first steps undertaken by the EU in this direction: BREVE (*Behavioural Responses to Privacy Visceral Notices*), a project recently launched by the European Commission, aims at studying the impact of different, innovative online privacy notices on users' behaviour as regards their privacy. The aim is to encourage also in Europe the use of behavioural research for policy making in the field of *privacy*.

In light of the above, this article is structured as follows: Part II briefly recalls the main findings of the current research on privacy policies and informed consent requirements as (ineffective) legal tools for privacy protection also in comparison with other information disclosure mechanisms (e.g., in consumer protection contexts). The starting point will be the analysis of the phenomenon called the "privacy paradox." Having learned the lessons from previous studies and experiments on users' practices online, Part III discusses the challenges and opportunities of behavioural sciences applied to public policy in order to better understand the relevance of behavioural aspects in the *privacy* area. The focus will be, eventually, on *privacy* information provisions and users' data disclosure behaviour, with particular emphasis on recent research conducted on *Privacy Visceral Notices*. Part IV, finally, provides some recommendations on how to integrate Behavioural Insights into privacy policy and law (hard law and/or soft law) and on future research. In this way, this paper seeks also to integrate that research strand that explores to what extent (and at what level of governance) the regulatory approach could play a role in cyberspace.[26]

---

24. Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCH. & PERSONALITY SCI. 40, 41-45 (2013).

25. *See, e.g.*, Victoria Groom & M. Ryan Calo, *Reversing the Privacy Paradox: An Experimental Study* 1 *passim* (Social Science Research Network, Working Paper, 2011) (experimental study on the efficacy of various techniques of nonlinguistic notice on consumer privacy expectations); Yang Wang et al., *A Field Trial of Privacy Nudges for Facebook*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2367 (2014) (reporting the results of an experiment conducted on U.S. students, users of Facebook and exposed to different privacy nudges, ranging from a "time nudge" to the "emotional nudge").

26. *See generally* Oreste Pollicino & Marco Bassini, *Internet Law in the Era of Transnational Law* (Robert Schuman Centre for Advanced Studies, Working Paper No. 24 (2011).

II. PRIVACY NOTICES AND PRIVACY PARADOX

A. *Information obligations and informed consent*

"Confidence in the Internet and its governance is a prerequisite for the realization of the Internet's potential as an engine for economic growth and innovation. . . . The [European] Commission is addressing these challenges, notably via the reform of the EU Data Protection framework."[27]

The Draft GDPR, to which this reform has been assigned, strengthens the consent requirement and the transparency principle, as said in the introduction: "The controller shall *have transparent and easily accessible policies*."[28] This information disclosure obligation is imposed by the European legislator to any data controller,[29] including Internet companies/ISPs: they should provide complete and accurate information regarding purposes, nature, conditions of online data processing and users' privacy rights, so that the subjects can provide an "aware" consent.[30]

---

27. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Internet Policy and Governance: Europe's Role in Shaping the Future of Internet Governance*, at 9, COM (2014) 72 final (Feb. 12, 2014) (EC).

28. *Proposal for GDPR*, *supra* note 2, at 47.

29. Data controller "determines the purposes, conditions and means of the processing of personal data," as far as there purposes are legitimate. *See id.* at 41-42.

30. The consent to data processing that the data subject might decide to give should refer also to the purposes for which personal data are processing. In the EU legislation, in fact, the consent is conceived as a major instrument for individuals to keep control over the processing (and the purposes) of their data. This also explains the relevance of the notion of free and specific consent as well as of 'further purposes' for which data might be processed. Interestingly, while the current Directive 95/46 states that data cannot be further processed in a way incompatible with the purposes for which they have been collected (Art 6), the Draft Regulation introduces a more permissible criterion. Further processing is allowed where the purposes are compatible with those for which the data have been collected (Art 6): i.e. in case of further processing, subject's consent is required only in case of incompatibility of the further purposes. Internet companies certainly receive advantage from this amendment, as they will not need to ask for consent in many 'compatible' cases. The purposes limitation principle has its equivalent in the North American privacy literature in the concept of 'contextual integrity' and possibly in its regulation as one of the principles of what will be the first U.S. general privacy Act. *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 J. AM. ACAD. OF ARTS & SCI. 32, 37 (2011); *see also* EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012). Although it does not seem to add anything new to the European legal framework, the *context integrity* principle could be a useful, interpretive instrument also for the application of the EU Draft DP Regulation, *e.g.* defining the limits of data processing for further purposes, and thus, the scope of the consent, especially online. *See* Kristina Irion & Giacomo Luchetta, *Online Personal Data Processing and EU Data Protection Reform*, CEPS TASK FORCE REP.

The traditional way to fulfill this obligation online is the provision of privacy notices (or policies). More precisely, privacy notices are statements that should help data subjects to understand how data controllers will use their personal data, providing them with detailed information about what, why and how personal data will be collected, processed, stored, used and in cases, disclosed. These notices should also provide information about the data subjects' rights (e.g., to access their personal data) and the security measures adopted for its safe treatment. The final goal would be to confer individuals with control over their personal data and, through this control, to allow them to decide for themselves how to weigh the costs and benefits of the disclosure of their data: this approach is also called "self-management privacy."[31]

These privacy notices have been gradually introduced as implementation of mandatory regulation (that is the rule in the EU) or adopted as self-regulation practices by businesses in response to privacy concerns (that is the rule in the U.S.).[32] Criticisms to the self-regulation model of privacy policies, in particular in the U.S., point out the fact that this model has allowed a sectorial and weak approach to privacy[33] all in favor of business interests. With a proliferation of privacy policies not accompanied by substantial safeguards, individual protection would have become more an appearance of privacy than a reality: users may believe they have more privacy simply because a website has a privacy policy,[34] or they are presumed to be consenting to a website's privacy conditions

---

CEPS DIGITAL FORUM (2013), *available at* http://www.ceps.eu/publications/online-personal-data-processing-and-eu-data-protection-reform (last visited Dec. 18, 2015).

31. Daniel Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1882 (2013).

32. While in the EU information obligations for companies and governmental entities dealing with data processing stem from general privacy legislations, at both *supra*national and national level, in the U.S. sectorial regulations and a self-regulation model prevail, as a federal legislation is missing and a State legislation on privacy is exceptional. *See, e.g.*, CAL. BUS. & PROF. CODE §§ 22575-79 (West 2015). For an overview on the increasing privacy concerns in U.S. (from 43% in the 1990 to 88% in 2003) and for a critical assessment of privacy policies use by companies see generally Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587, 592, 624 (2007) (claiming that U.S. privacy policies, far from being an instrument of protection, have become one more adhesion contract for individuals to avoid, the enforcement of which might be challenged by individuals at least for "(1) a lack of *assent*, as many online privacy policies still employ browse-wrap acceptance features; and (2) unconscionability of terms"). *See also* Chris J. Hoofnagle et al., How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? 20 (Apr. 14, 2010) (unpublished manuscript) (on file with the U.C. Berkeley School of Law, Berkeley Center for Law and Technology).

33. Daniel Solove & Chris J. Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 357, 365-66 (2006).

34. Haynes, *supra* note 32, at 610.

simply because they are visiting that website and using its services.[35]

In Europe, the adoption of privacy policies derives from the implementation of general Data Protection principles and rules (mainly, fairness and information obligations). However, traditional privacy policies (or notices) are criticized also in Europe as they proved to be insufficient to realize the purposes of data protection. Despite the theoretical value of privacy policies, the efficacy of current notice and consent mechanisms is increasingly questioned in the privacy area,[36] as well as in other areas, so much that someone has defined certain criticisms, at times excessive, "notice skepticism."[37]

Traditional privacy policies tend to be written, detailed and usually long and highly complex texts; in online environments, they consist of separate texts hardly accessible or displayed in a slightly visible part of a website. Internet users are asked to consent to the conditions described in the privacy policies by ticking a "yes" box at the end of the statements; more often, this box is simply positioned beside a link (hyperlink), which refers to another page (hypertext) containing the privacy policy: clicking the box presumes you have read the policies.

Users are supposed to read these texts, understand them and give their informed consent to the processing of their personal data along the lines explained in the privacy policies. Nevertheless, this assumption is—most of the time—flawed, as data-subjects tend to merely scroll down the privacy policies and rush for the tick box (or simply tick the box without even following the link).

By providing these textual information notices, however, data controllers comply, at least formally, with their information obligations. Like for other disclosure obligations (e.g., on products and services

35. For an overview on advantages and disadvantages of privacy ("Having too much privacy can be as bad as having too little") see Lior J. Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2010, 2039, 2041 (2013), who talks of distributive effects of privacy (it benefits some people and damaged others) and urges, also for the U.S., a more proactive and non-sectorial way to protect privacy.

36. *See* Brendan Van Alsenoy et al., *Privacy Notices Versus Informational Self-Determination: Minding the Gap*, 28 INT. REV. L. COMPUTERS & TECH. 185 (2014); Brendan Van Alsenoy & Alessandro Acquisti, *Privacy-Friendly 'Model' Privacy Policies*, SECURITY AND PRIVACY FOR ONLINE SOC. NETWORKS (2013), *available at* https://lirias.kuleuven.be/bitstream/123456789/453694/1/SPION_D9.3.5_Privacy_friendly_model_privacy_policies.pdf (last visited Dec. 18, 2015); *see also* Alessandro Mantelero, *The Future of Consumer Data Protection in the E.U. Re-thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, 30 COMPUTER L. & SECURITY REV. 643 (2014).

37. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1055-57 (2012).

quality as set in the Consumer Protection regulation[38]), in fact, the European data protection law does not specify the format that this information to be provided to the users should have[39] (or provides only few indications). This means that, as far as the information provision obligations are satisfied, i.e., the minimum of information required by data protection rules has been provided, the controller is free to choose the way to provide this information, regardless of its effectiveness.

1. *Role of privacy policies in users' data disclosure*

The role of privacy policies should be also to enable in the users a cautious and aware *willingness to disclose* personal data.[40] Under an economic perspective, willingness to disclose personal data might be beneficial for companies (increasingly relying on an information-based business model) and, to some extent, also for the users, who might have personalized, higher quality services and relevant promotions.[41] It would be about striking a balance between obtaining advantages of targeted services and keeping control over their own personal data. According to the neoclassic economic view of privacy, individuals would "rationally" trade off their short term benefits (e.g., targeted services) and long terms costs of data disclosure (e.g., risks of privacy invasion), being able to make a pondered decision.

Some scholars have shown the relationship between the content of privacy policies and the users' intention to interact with websites where there is a requirement to provide personal data.[42] Privacy concerns seem to have a negative impact on the willingness to provide personal information, while trust seems to have a positive impact. However, if people see benefits of disclosure (like personalized services in e-commerce or entertainment in social networks) as outweighing the concerns for privacy risks, they would be more likely to disclose. Given that willingness to provide personal data online is closely related to privacy concerns, a way to reduce these concerns would be to provide them with good privacy policies, i.e., with really informative policies, increasing users' awareness and reassuring them about possible risks:[43] the information would be able to reduce privacy concerns and to increase

38. Consumer protection in Europe is now enshrined in the European Directive on Consumer Rights 2011/83/EC. *See* Council Directive 2011/83, 2011 O.J. (L 304) 64 (EU).

39. Some indications, however, have been offered by the *Opinion on the Definition of Consent*, *supra* note 14, at 26.

40. *Proposal for GDPR*, *supra* note 2, at 8, 25.

41. Wu et al., *supra* note 21, at 890.

42. *Id.* at 891.

43. *Id.*

trust in websites. In other words, using privacy policies, which clearly inform users about how companies treat their data and which are read by users, according to Wu et al., would not only reduce their concerns and increase trust, but it would meanwhile increase users' willingness to disclose personal information.[44]

However, things seem more complicated than they have just been pictured; reducing privacy concerns through complete information is not enough to increase trust. Other studies have shown, in fact, that often the greater the privacy reassurances provided to individuals, the greater their reluctance to reveal personal information because the strong privacy reassurance primes the individuals about the sensitivity of their data. [45]

Moreover, it does not guarantee a safe digital environment for individuals, to whom a cautious, responsible behaviour is required (regardless of the duly supervisory role of regulatory authorities). Risks of privacy violation, illicit data practices or violations of correlated rights (e.g., to non-discrimination, etc.) deriving from the increasing reliance on Big Data became a worrying reality in the digital era.[46] Education and good information are certainly important but demonstrated not to suffice.[47] Therefore, restrictive legal intervention is sometime deemed necessary to protect the data-subject, usually the weakest party in online and offline relationships.

In the attempt to curb the risks for data protection (and related concerns) arising from the massive use of digital technologies, the EU Draft DP Regulation not only strengthens some of the existing safeguards—like the information obligations for data controllers—but also reaffirms the principle of minimization of data collection and processing.[48] On the one hand, personal data collection by public and private entities is not forbidden by the EU law, but regulated and structured; on the other, personal data disclosure by users is not

44. Wu, *supra* note 21.

45. Alessandro Acquisti, *The Economics of Personal Data and the Economics of Privacy: 30 Years after the OECD Privacy Guidelines* 13 (Working Party for Info. Security & Privacy & Working Party on Info. Econ., Background Paper No. 3, 2010), *available at* http://www.oecd.org/sti/ieconomy/46968784.pdf (last visited Dec. 18, 2015).

46. *See, e.g.*, *Opinion of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on "Purpose Limitation"* (Apr. 2, 2013), *available at* http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf (last visited Dec. 18, 2015); Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. 25 (2013).

47. Hoofnagle et al., *supra* note 32, at 20.

48. *See Proposal for GDPR*, *supra* note 2, at 22. "The data should be *adequate*, *relevant and limited to the minimum necessary* for the purposes for which the data are processed; this requires in particular ensuring that the data *collected are not excessive* and that the period for which the data are stored is limited to a strict minimum." *Id.* (emphasis added).

discouraged, yet driven to be more aware and wise.

2. *Personal data disclosure: direct and indirect*

It is important to stress that personal data disclosure (and its specular activity, data collection) might occur inadvertently, especially online, where most of people's daily activities are nowadays performed. During their browsing, people leave continuous traces of their behaviour, private lives and preferences without being asked, or without being aware. Data disclosure, in fact, might be direct, i.e., on a *voluntary* basis (like in the cases of filling in an online form) and indirect, as a result from other online activities (web browsing, location moving, click stream, etc.).[49] The latter kind of data disclosure/data collection may create more concerns as it may occur unobtrusively, out of users' control. Most of the time, the two kinds of data collection are also combined: data collected "indirectly" might be matched with data of direct disclosure, allowing companies or public organizations to have a complete profile of people.

Wide literature exists about the several issues raised by profiling techniques[50] and by the "hidden" collection of data, not least the fear of mass surveillance[51] and users' manipulation. Now, the problem is that against this indirect disclosure, traditional privacy notices have very little or any effect at all.[52]

3. *Data disclosure between individual autonomy and legal constraints.*

In certain cases, the individual's autonomy to choose whether or not to disclose their data is restricted by the law intervention, regardless of users' informed consent, because it is presumed not freely given, not genuine and therefore not valid.[53] Some privacy risks are deemed so

---

49. *See generally* Groom & Calo, *supra* note 25.

50. *See generally* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINE PERSPECTIVES (Mireille Hildebrandt & Serge Gutwirth eds., 2008). The Draft GDPR takes into account new scenarios, acknowledging the existing practices of users profiling as new business models for companies but also introducing specific limitations to them.

51. *See, e.g.*, Roger Clarke, *Profiling: A Hidden Challenge to the Regulation of Data Surveillance*, 4 J.L. & INFO. SCI. 403 (1993); Roger Clarke, *Information Technology and Dataveillance*, 21 COMM. OF THE ACM 498 (1988).

52. *See generally* Groom & Calo, *supra* note 25.

53. The EU law intervenes to prohibit the collection and processing of special categories of data, even in the presence of individual's consent and when the conditions do not allow the individual to "freely" choose to consent. *See Proposal for GDPR*, supra note 2, at 22. "In order to ensure free consent, it should be clarified that consent *does not provide a valid legal ground* where the individual *has no genuine and free choice* and is subsequently *not able to refuse* or withdraw consent without detriment." *Id.* (emphasis added).

Consent should not provide a valid legal ground for the processing of personal data,

serious by the EU legislation to foresee a strong protection especially for weaker categories of people.[54]

This limitation to individual autonomy, especially in contractual context, which might appear an excess of paternalism, can be explained by the status of data protection and privacy as fundamental rights.[55] This approach has been strengthened with the entry into force of the Treaty of Lisbon in December 2009 that gave to the Charter of Fundamental Rights of 7 December 2000 ("CFR") a binding force of primary law in the EU.[56]

Pursuing the economic development (also) by fostering the free flow of personal data, the European DP law aims at the "protection of individuals with regard to the processing of personal data."[57] Privacy and data protection is understood in Europe as not only an individual right, but also as a public interest, a *conditio sine qua non* for a democratic society, a liberty rather than a freedom:[58] essential to guarantee the right to self-determination, it would ensure other rights, like freedom of expression, enable diversity and prevent undue societal control.[59]

> where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.

Id.

54. *See id.* at 45. Article 8 sets out further conditions for the lawfulness of the processing of personal data of children in relation to information society services offered directly to them.

55. On a discussion on the private law approach to personal data protection see generally Nadezhda Purtova, *Private Law Solutions in European Data Protection: Relationship to Privacy and Waiver of Data Protection Rights*, 28 NETH. Q. HUM. RTS., 179 (2010).

56. As recalled above, the Charter contains two separate articles for privacy right and for data protection rights. Charter of Fundamental Rights of the European Union, art. 7-8, Dec. 18, 2000, 2000 O.J. (C 326) 1. Moreover, article 16 of the Treaty on the Functioning of the EU provides now the legal basis for any piece of legislation adopted by the EU on data protection. Consolidated Version of the Treaty on the Functioning of the European Union art. 16, May 9, 2008, 2008 O.J. (C 115) 47, 55.

57. *See* Council Directive 95/46, 1995 O.J. (L 281) 31 (EC); *see also Proposal for GDPR*, *supra* note 2, at 2.

> It is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities.

Id.

58. *See generally* Antoinette Rouvroy & Yves Pullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, *in* REINVENTING DATA PROTECTION 45 (Serge Gutwirth et al. eds., 2009).

59. *See generally* Mireille Hildebrandt & Bert-Jaap Koops, *The Challenges of Ambient*

Although many times the two statuses overlap, the concept of data subject or user does not coincide necessarily with that of the consumer,[60] as well as the European DP law is not a consumer protection law.[61]

Legal public intervention and supervision mechanisms in favor of individuals' privacy, which might take place regardless of the interested subject's consent to data processing, are not rare in Europe, and are aimed at verifying that other legal grounds (e.g., necessity, proportionality) occur: this is not only to overcome the limitations of a merely self-regulating approach to privacy,[62] but also to guarantee the same existence of democratic processes.[63]

This public intervention, foreseen by the *sui generis* EU Data Protection law[64] to protect the individual's rights, may occur to limit market practices that might jeopardize individuals' rights. The regulatory intervention may take place by imposing information disclosure requirements to companies that collect data, as well as conditions and limitations to the validity of a subject's consent (presumed not valid in cases of children or in cases of unbalanced decisional powers in the employment area).[65] It is also reflected in the decisional, monitoring and

---

Law and Legal Protection in the Profiling Era, 73 MOD. L. REV. 428 (2010).

60. For considerations on the consequences of this approach on the legal nature of data subject consent, as unilateral act, like an authorization rather than as a contractual agreement, see Daniel Le Metayer & Shara Monteleone, *Automated Consent Through Privacy Agents: Legal Requirements and Technical Architecture*, 25 COMPUTER L. & SECURITY REV. 136, 138 (2008). The issue, however, is debated in literature, reflecting two different approaches to Data Protection mainly embraced in EU the first, mostly followed in U.S., the second.

61. *See* Irion & Luchetta, *supra* note 30, at 21-22. This Report also stresses the difference between DP and consumer protection, which refers to a cross-cutting EU policy field that aims at enhancing the positions of consumers of product and services; however, according to Irion & Luchetta (CEPS)'s Report, consumer protection regulation when modifies contract law to the benefit of the consumer (*e.g.* regarding unfair terms and practices) would depart from the party autonomy principle, while DP framework would strongly emphasizes the control and autonomy of individual through the instrument of consent. Although I fully share the view of consent as enabling individual to control over her data, I would stress the idea that the European DP regulation contains as much limitations to individual autonomy, deemed necessary for protecting a fundamental right like data protection that is also an essential public interest. First because the consent does not legitimize every type of data processing and also because the interest of data subject is at the center of the European legal framework (even more in the ongoing reform) so much that the protection of his data and private sphere may be acknowledged and granted despite his consent to data collection and regardless of whether he issued a complaint or not. *See generally* Le Metayer & Monteleone, *supra* note 60.

62. Solove & Hoofnagle, *supra* note 33, at 385.

63. *See, e.g.*, Rouvroy & Poullet, *supra* note 58; Julie E. Cohen, *Privacy and Technology: What Privacy is For*, 126 HARV. L. REV. 1904, 1912 (2013).

64. Irion & Luchetta, *supra* note 30, at 22.

65. *See Proposal for GDPR*, *supra* note 2, 43-45.

sanctioning powers granted by the EU law to DP national authorities.[66] The latter could intervene, even *ex officio* (i.e., without a formal claim by the interested subject) to adopt the needed legal measures, aimed at preventing, forbidding data processing detrimental for individual rights or remedying its consequences.[67]

This rights-based approach is also reflected in the recent case law of the European Court of Justice ("ECJ")[68] and seems confirmed by the Draft GDPR; conditions and bans on the use of personal data have been strengthened, at the risk of being considered paternalistic. However, a defensive approach to data protection and privacy rights does not need to be also too rigidly paternalistic.

As discussed below, a different, "soft" perspective seems possible, as well as an evolving interpretation of the DP rules, which, backed by an integrated system of alternative regulatory mechanisms, namely appropriate *nudging* strategies, would allow data protection while preserving the individual autonomy.

4. *Limitations of the current safeguards: the privacy paradox*

Given the relevance of informed consent for data protection, one could expect that it suffices to strengthen these information obligations and foster the provision of privacy policies to enable users to give a meaningful, informed consent.[69]

The proposed GDPR reinforced this concept; however, the reality has shown that this still valuable mechanism is not working well in practice, especially in the digital world.

One of the main criticisms to the informed consent requirement relates to the weakness of the link between information about data processing and consent and to the incapacity of consent to provide

66. *Id.* at 77-78.

67. *See id.* at 77-80.

68. As examples of application of this rights-based approach see Case C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España S.A.U., 2008 E.C.R. I-00271 (Jan. 29, 2008); Case C-70/10, Scarlet Extended S.A. v. Société belge des auteurs, compsiteurs et éditeurs S.C.R.L. (SABAM), 2011 E.C.R. I-11959 (Nov. 24, 2011); Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 EUR-Lex CELEX LEXIS 317 (May 13, 2014).

69. Although strictly connected, information obligations and informed consent are separate concepts and requirements. Transparency principle (and consequent information obligations) apply also in case of derogations from the consent requirements. This is particularly relevant in all those cases in which it might be impossible to systematically collect users' consent, but that still require the fulfilment of transparency principle about how data are processed. *See* Mireille Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, *in* DIGITAL ENLIGHTENMENT YEARBOOK 41 (Jacques Bus et al. eds., 2012).

effective control to users over their data.[70]

While Internet users usually declare to be worried about online privacy risks and to be aware of their privacy rights, in fact, the analysis of their online behaviour and attitudes, in terms of personal data disclosure, seems to suggest that they do not care about privacy. From the Special Eurobarometer 359/2011 of the European Commission ("EB"),[71] emerges that the majority of Internet users report to read these privacy notices when joining a social network or registering for a service online.[72] However, most users' online behaviour shows that they do not act according to their statements, as they do not read the privacy policies entirely or they find it difficult to obtain information about a website's data practices.[73] A large number of people are, nevertheless, concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.[74] Similar surveys[75] seem to confirm this attitude.[76]

In sum, even when people declare to be worried about their privacy, they do not read privacy policies and do not stop disclosing their data, and even when people declare to read these notices they do not seem to reduce privacy concerns. This phenomenon is also called as "the privacy paradox"[77] and has led to questioning the adequacy of the current privacy and data protection mechanisms. The idea that people do not care about their privacy, however, appears too simplistic in light of the most recent research and it has been discarded by most privacy scholars.[78]

---

70. Irion & Luchetta, *supra* note 30, at 48.

71. *See Report of the Directorate-General of Justice, Information Society & Media and Joint Research Centre on Attitudes on Data Protection and Electronic Identity in the European Union*, at 137 (June 2011), *available at* http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (last visited Dec. 18, 2015) [hereinafter *Attitudes on Data Protection*].

72. *Pan-European Survey of Practices*, *supra* note 18, at 1.

73. Tsai et al., *supra* note 22, at 17-18.

74. *Id.* at 1.

75. *See* Lee Raine, Aaron Smith & Maeve Duggan, *Coming and Going on Facebook*, PEW RES. CTR. 2 (Feb. 5, 2013), *available at* http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Coming_and_going_on_facebook.pdf (last visited Dec/ 18, 2015). For a user survey in mobile context (*e.g.*, about the consent provision in the use of Apps by young students) *see generally* Yue Liu, *User Control of Personal Information Concerning Mobile-app: Notice and Consent?*, 30 COMPUTER L. & SECURITY REV. 521 (2014).

76. Tsai et al., *supra* note 22, at 254. *See also* Hoofnagle et al., *supra* note 32, at 3.

77. *See Pan-European Survey of Practices*, *supra* note 18, at 16, 47, reporting and building upon the European Commission's discussion of the *Special Eurobarometer 359/2011*. *See Attitudes on Data Protection and Electronic Identity in the European Union*, *supra* note 71, at 112-15.

78. *See, e.g.*, Hoofnagle et al., *supra* note 32, at 3-4; Danah Boyd & Alice Marwick,

Studies have shown that the reasons for the limitations of informed consent and privacy notices should be ascribed, first of all, to the lack of sufficient information for the users to make a pondered decision about data disclosure, that is, an accurate cost-benefit analysis.[79] This is also called information asymmetry between users (they are unaware or they do not have enough information on what happens with their data) and data controllers (companies or governmental entities that collect and process users' data).[80] This knowledge asymmetry suffered by users about further use of data is particularly sharpened on the Internet, where it is easier to collect data and where "Big Data is poised to reshape the way we live, work and think."[81] The characteristics of Big Data as new technological trend and the entities capable to handle the power of knowledge deriving from it are unknown to most of people, who often do not have (or see) alternatives to consent to their data collection. In the mobile context, then, the lack of meaningful choice to consent to the use of Apps is even more evident when someone talks about the subject's consent as "blind consent."[82]

Regulators tried to cope with this asymmetry, imposing stricter information requirements to data controllers before (or contextually to) the collection of data as transparency mechanisms (like privacy notices).

Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies 1-29 (Sept. 2011) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128 (last visited Dec. 18, 2015); Norberto Andrade & Shara Monteleone, *Digital Natives and the Metamorphosis of the European Information Society. The Emerging Behavioral Trends Regarding Privacy and Their Legal Implications*, *in* EUROPEAN DATA PROTECTION: COMING OF AGE 119, 120 (Serge Gutwirth et al. eds., 2013).

79. Acquisti, *supra* note 45.

80. *See* Frederik J. Zuiderveen Borgesius, *Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics?* 3 (July 27, 2013) (Amsterdam Law School, Research Paper No. 2013-43), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2300969 (last visited Dec. 18, 2015), who stresses that users do not know how their data will be treated and even if they knew, they ignore the consequences of future data use. As he notices, this information asymmetry (and in particular the lack of knowledge about the economic 'value' of own data) would be also the reason why consent within Data Protection regime cannot be considered only under the economic perspective, as a trade-off between 'two parties', an exchange of free service v. personal data. Another reason, however, may be *see*n in the legal significance of data protection as a public interest in a democratic society, from which a different consideration of consent would stem: its nature would be seen as authorization (like an administrative act) rather than as a contractual agreement). *See* Le Metayer & Monteleone, *supra* note 60, at 137.

81. Kennet N. Cukier & Viktor Mayer-Schoenberger, *The Rise of Big Data*, FOREIGN AFFAIRS (May 2013), *available at* http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data (last visited Dec. 18, 2015).

82. Liu, *supra* note 75.

The assumption is that if users receive appropriate and clear information, they will be able to take a pondered decision about consenting or not to their data processing by, for instance, a website or Social Network: this may include the installation of cookies on one's own device.[83]

However, even if complete and detailed information is provided by data controllers,[84] studies have proved that current privacy notices are not effective: they fail to help data subjects in their decision-making and consequent behaviour as regards to their data disclosure. Traditional privacy policies are "hard to read, read infrequently, and do not support rational decision-making."[85]

Information asymmetries seem difficult to solve, as people are discouraged to read privacy polices (and thus interpret them in their favor): transactional costs (namely the time needed for users to read and interpret them, in case complete information is provided) would make this information asymmetry even more difficult to overcome.[86] In addition, users have to face increasing uncertainty in online environments due to new technological capabilities of tracking systems, with information being gathered in different ways and by new actors: lacking common standards, privacy policies change frequently (though not always clearly) in order to include these upgrades, making the task of keeping abreast with the recent version even more difficult for users.[87]

Some scholars go even further, claiming that even well-informed and rational individuals could not appropriately self-manage their privacy due to several structural problems: a) there would be too many entities collecting and using personal data to make the self-management system (i.e., consent) feasible and b) many privacy harms would be the result of

---

83. *See* Council Directive 2002/58 2002 O.J. (L 201) (EC) as modified by Council Directive 2009/136, 2009 O.J. (L 337) (EC) (*cookies* Directive). For a recent overview on *functional* and *not functional* cookies, see Joasia Luzak, *Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy*, 37 J. CONSUMER POL'Y 547, 547-49 (2014).

84. That is assuming companies' fairness in providing true information. Whether companies are not faithful to their privacy policies is, rather, an accountability issue, a matter that goes beyond the scope of this paper. However, it must be noted that further use of data by third parties is often deliberately not covered by a privacy policy, so that companies are exempted from responsibility of third party's processing of data.

85. McDonald & Cranor, *supra* note 19, at 541.

86. Acquisti & Grossklags, *supra* note 22, at 372; McDonald & Cranor, *supra* note 19, at 546; Borgesius, *supra* note 80, at 31.

87. Kirsten Martin, *Transaction Costs, Privacy and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online*, 18 FIRST MONDAY (Dec. 2, 2013), *available at* http://firstmonday.org/ojs/index.php/fm/article/view/4838/3802 (last visited Dec. 18, 2015).

an aggregation of pieces of data by different entities.[88] Therefore, the current privacy self-management "which takes refuge in consent,"[89] through the notice and choice mechanism, does not seem to provide people with meaningful control over their data.

The 'notice and choice' mechanism is especially popular in the U.S., but similar considerations can be made in the EU as far as informed consent is required to process personal data.

B. *Addressing the drawbacks: alternative mechanisms to traditional privacy policies*

1. *A legal-technical approach*

The privacy paradox emerging from users' attitudes and behaviour online, might be explained in terms of lack of suitable and flexible legal-technical instruments for users to safeguard their privacy, while they seek to enjoy the advantages of innovation and technology.[90]

Attempts to address this lack are not missing, especially in multidisciplinary research environments, where scholars, since at least two decades, have pointed out the need to achieve a more integrated legal-technical approach to privacy.[91] The main idea is that many privacy concerns and legal implementation issues might be addressed through a good technical design that embeds fundamental privacy principles—better known as the privacy by design approach ("PbD").[92] Privacy

88. Solove, *supra* note 31, at 1888-89.

89. *Id.* at 1880.

90. A point that emerges from these surveys is that users (and in particular the youngsters, so called 'Digital Natives') when dispose of adequate mechanisms to avoid privacy risks they make better decisions or they create their own strategies. *See Pan-European Survey of Practices*, *supra* note 18; *see also* Boyd & Marwick, *supra* note 78.

91. *See, e.g.*, Yves Poullet, *Pour une Troisième Génération de Réglementations de Protection de Données*, 3 JUSLETTER (2005); Mireille Hildebrandt, *Legal and Technological Normativity: More (and Less) than Twin Sisters*, 12 TECHNÉ: RES. PHIL. TECH. 169 (2008); ANDREW MURRAY, INFORMATION TECHNOLOGY LAW: THE LAW AND SOCIETY (2d ed. 2010). On the concepts of "Transparency Enhancing Technologies," allowing citizens to possibly anticipate how they will be profiled and the consequence of that see Gordon Hull et al., *Contextual Gaps: Privacy Issues on Facebook*, 13 ETHICS & INFO. TECH. 289 (2011); Shara Monteleone, *Privacy and Data Protection at the Time of Facial Recognition: Towards a New Right to Digital Identity?*, 3 EUR. J. L. TECH. (2012). *See* Hildebrandt, *supra* note 69, at 52-59.

92. *See, e.g.*, Ann Cavukian, *Privacy by Design and the Emerging Personal Data Ecosystem*, PRIVACY BY DESIGN (Oct. 2012), *available at* http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf (last visited Dec. 18, 2015). This approach was formally embraced in 2010 by Privacy Commissioners at their 32nd International Conference, in Jerusalem, where an ad hoc Resolution was adopted. *See Resolution on Privacy by Design*, 32D INT'L CONF. DATA PROTECTION & PRIVACY COMMISSIONERS (Oct. 27-29, 2010), *available at*

enhancing technologies ("PET"), based on specific technical settings that embed privacy principles, proved to play a relevant role in support of privacy and data protection.

The European Commission has been promoting for years legal-technical measures at safeguard of these rights, as essential tools for building confidence online. The Draft GDPR now formalizes the *Data Protection by design* and *by default* principles, introducing specific norms and constraints (Article 23). The close and complex relationship between ICTs and public policy became particularly evident with the development of the Internet and of the Information Society. As stressed in the recent EC Communication on Internet Governance:[93] "Technical details of Internet protocols and other information technology specifications can have significant public policy implications. Their design can impact on human rights such as users' data protection rights and security, [and] their ability to access diverse knowledge and information . . . ." The Commission, although welcomed the efforts of the international technical community to establish approaches to specification setting based on public policy concerns,[94] acknowledged that key decisions are frequently made by technical experts in the absence of efficient mutual interactions between technical and public policy considerations.[95] "This is particularly important when legal rights of individuals, especially their human rights, are clearly impacted."[96]

Special attention should be paid in the design of specific Internet

---

http://privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J5.pdf (last visited Dec. 18, 2015).

93. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, International Policy and Governance Europe's Role in Shaping the Future of Internet Governance*, at 4, 8-9, COM (2014) 72 final (Dec. 2, 2014) [hereinafter *Shaping the Future of Internet Governance*].

94. *Internet Governance Principles*, NETMUNDIAL (Apr. 23-24, 2014), *available at* http://content.netmundial.br/contribution/internet-governance-principles/176 (last visited Dec. 18, 2015). Positive examples include recent technical guidance for privacy considerations in new protocols. See the guidelines elaborated by the Internet Architecture Board (IAB), Cooper et al., *Privacy Considerations for Internet Protocols*, INTERNET ARCHITECTURE BOARD (July 2013), *available at* http://tools.ietf.org/pdf/rfc6973.pdf (last visited Dec. 18, 2015), which are a development of many sets of privacy principles (like the Fair Information Practices and the privacy by design frameworks that have been developed in different forums over the years). Interestingly, in the recent IAB's guidelines, user participation and interaction is taken into account.

95. These considerations seem to be at the basis also of the European Commission Decision of 28 November 2011. *See* Commission Decision of 28 November 2011 on Setting up the European Multi-stake Platform on ICT Standardisation, 2011 O.J. (C 349) 4, in which a plurality of different actors are called to contribute to the definition of the ICT standardization.

96. *Shaping the Future of Internet Governance*, *supra* note 93, at 9.

architecture, especially with the advent of new digital and smart technologies, given that normativity of technology may be as relevant and effective as the normativity of law (though different) and have an impact on human behaviour and conduct.[97] Moreover, the adoption of ad hoc legal-technical measures to improve the level of transparency online like "Transparency Enhancing Technologies" ("TETs") is also urged.[98] Most users are not even aware that their data are collected or that they are being tracked and profiled while surfing the web[99]: enhanced transparency might help individuals to understand how their personal data are used and what the potential dangers are. Given that information flows are growing dramatically, TETs might be critical.[100] The increase of transparency (on how the data are used) and the availability of easy-to-use privacy-control mechanisms are considered essential aspects in order to ensure a sustainable flow of data that makes privacy to be a virtue for both business and users:

> [While transparency] might initially reduce sharing, it limits the risk of brand damage and helps to attract more informed customers. . . . [P]rivacy controls should be available and easy to use. They will significantly increase data-sharing by individuals, likely offsetting any negative impact on sharing resulting from increased transparency.[101]

Methods of providing information and offering the right to refuse should *be as user-friendly as possible*. This seems to stem from the e-Privacy Directive[102] and also from the draft GDPR (Article 11).[103] Therefore, companies should go beyond the drafting of long and complex privacy policies as the most suitable way to inform users about processing of their own data and it would be also in their own interests to resort to alternatives to traditional notice and choice mechanisms in order to increase trust in online practices. Consequently, rather than only using

97. *See* Hildebrandt, *supra* note 69; *see also* HUMAN LAW AND COMPUTER LAW: COMPARATIVE PERSPECTIVES (Mireille Hildebrandt & Jeanne Gaakeer eds., 2013).

98. Hildebrandt, *supra* note 69.

99. *See generally* Borgesius, *supra* note 79; Hildebrandt & Koops, *supra* note 59.

100. *See* Claude Castelluccia & Arvind Narayanan, *Privacy Considerations of Online Behavioural Tracking*, EUR. UNION AGENCY FOR NETWORK & INFO. SECURITY (Oct. 19, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking (last visited Dec. 18, 2015).

101. *The Value of Our Digital Identity*, Boston Consulting Group 17 (2012), *available at* http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (last visited Dec. 18, 2015).

102. *See* Council Directive 2002/58, 2002 O.J. (L 201) (modified by Council Directive 2009/136/EC).

103. *Proposal for GDPR*, *supra* note 2, at 47.

written privacy policies that the majority of users do not read, companies should engage into alternative ways and instruments—more visual, explicit, simple and user-friendly—to inform Internet users and help them make aware decisions.

Among the remedies identified in literature to cope with the "laudable goals and ultimate failure of notice and choice to respect privacy online,"[104] we can find in particular suggestions aimed to: (1) ameliorate the current notice and choice structure through opportune legislation, industry best practices and privacy enhancing technologies; (2) given the limited users' empowerment due to information asymmetry and transaction costs, focus on privacy reputation and trust, built by companies around respecting privacy expectations;[105] and (3) building on a stream of privacy scholarship that looks at a tort-law model of privacy protection,[106] develop privacy rules by identifying specific *harms* and consequences of data disclosure. The underlying idea is a shift from the notification scheme to managing privacy expectations within a specific *context*: a consequence-based approach to privacy that would be more pragmatic and beneficial also for companies than the current notice and choice, as the privacy norms would be constructed thinking to the harms and not to abstract risks of privacy violations.

Legal-technical proposals to solve the problem of the burdensome requirement of consent also include software personal agents, as an automatic way to achieve the protection of privacy. The underlying idea is that a technological architecture based on "Privacy Agents," which meets a series of legal requirements to ensure the validity of consent delivered through such an agent, could be useful to avoid overwhelming the data subject with repeated requests of consent, while protecting his/her privacy by respecting pre-settled preferences.[107]

Similar measures may be included amid all those technical solutions that embed and implement specific legal rules, also known as techno-regulation.[108] In Ambient Intelligence contexts such as *smart*

104. Martin, *supra* note 87.

105. In particular, according to Martin, firms have multiple tools at their disposal to meet privacy expectations, through three options: increase the obscurity of data exchange so to decrease the probability that information will be leaked; decrease the possible harm that could come from a leakage by using 'do not use' rules, limiting the use of data; increase the benefits of information exchange (possible uses of data) for individuals and society). *Id.*

106. *See, e.g.*, Ryan Calo, *The Boundaries of Privacy Harms*, 86 IND. L.J. 1131 (2011); Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DÆDALUS, J. AMERICAN ACAD. ARTS & SCI. 32 (2011).

107. Le Metayer & Monteleone, *supra* note 60.

108. Bibi van der Berg, *Colouring Inside the Lines: Using Technology to Regulate Children's Behavior Online*, *in* 24 INFORMATION TECHNOLOGY & LAW SERIES: MINDING

environments/cities (so called due to the capability of the sophisticated computer systems used to mine masses of personal and not personal data), TETs would allow citizens to anticipate how they will be profiled and which consequences this may entail.[109] However, the complexity and quantity of information produced by transparency enhancing technologies could overwhelm individuals, if this information were provided in the form of text, requiring their conscious attention:

> TETs will only succeed in empowering citizens if . . . [they do] not inundate a person with detailed technical information that requires her scrutiny in a way that nullifies all the 'advantages' of ubiquitous and seamless computing. . . . [They] will have to communicate the relevant information in a way that allows one to have 'a feel' of the environment's interpretation of one's behaviour, rather than merely adding more text or graphs to the equation.[110]

That is to say that even and primarily in the imminent digitalized and automated world, complementary mechanisms should be promoted in order to ensure that improved information about data processing is provided to the users. Layering of notice may be a step in this direction: data controllers may distribute the required information over different and progressive layers, such as, the short notice, the condensed notice and the complete notice.[111] In general, better ways of presenting information to people, short messages together with educational programs may mitigate inconvenience.[112]

However, providing simplified, standardized privacy information, although of some benefits, has proved to be also insufficient (e.g., cookies alerts): users might end up simply ignoring them and accepting all the requests of consent, by clicking on numerous message boxes.[113]

Nevertheless, it seems that "there is no limit to the ways in which

---

MINORS WANDERING THE WEB: REGULATING ONLINE CHILD SAFETY SERIES 67-84 (Simone van der Hof et al. eds., 24th ed. 2014); *see also* Ryan Calo, *Code, Nudge or Notice?*, 99 IOWA L. REV. 773 (2014).

109. Hildebrandt, *supra* note 69, at 53.

110. *Id.* (stressing that this, however, does not mean that a more precise access to the technical details must not be available, for instance to enable a person being subjected to unfair decision making on the basis of automatic profiling, to contest the application of profiles in a court of law).

111. *Opinion of the Data Protection Working Party on "More Harmonised Information Provisions"* (Nov. 25, 2004), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf (last visited Dec. 20, 2015); Brendan Van Alsenoy, *Privacy-friendly 'model' privacy policies*, SECURITY & PRIVACY IN ONLINE NETWORKS PROJECT [SPION] (June 2013), *available at* https://www.cosic.esat.kuleuven.be/publications/article-2363.pdf (last visited Dec. 20, 2015).

112. Luzak, *supra* note 83, 553-54.

113. Groom & Calo, *supra* note 25, at 8.

transparency and autonomous decision-making can be stimulated. Future research efforts should continue to seek out additional mechanisms to enhance transparency, both on ex ante and post fact basis."[114] Therefore, instead of rejecting tout court the notice and consent mechanisms as not effectively implementing the transparency principle, we should try understanding the underlying reasons, the actual users' attitudes and behaviours and seek out alternative, innovative and integrated ways to enhance them.[115]

2. *An integrated behavioural economic approach*

PbD approach and TETs are supposed to increase user's control over his personal data. However, advanced technical control mechanisms, though necessary, might not be sufficient if relevant cognitive and behavioural "biases" in online users are not taken into account:[116] several hurdles in privacy decision-making, in fact, have been highlighted by behavioural science.[117]

Empirical and social science research demonstrates that "there are severe cognitive problems that undermine privacy self-management. These cognitive problems impair individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data."[118] In other words, it is not enough having complete information about costs and benefits of disclosing personal data, as other factors intervene on the user's privacy choice and behaviour.[119] This line of enquiry has significant policy implications: as it has been noticed, "the modern microeconomic theory of privacy suggests that, when consumers are not fully rational or in fact myopic, the market equilibrium will tend *not* to afford privacy protection to individuals, and therefore privacy regulation may be needed to improve consumer and aggregate welfare."[120]

This seems particularly important if we consider how people think and act in the online environment: individuals' cognitive limitations mentioned before as regards information explain the failure of the rational choice model and of the informed consent (in the U.S., the "notice and choice" model) as regulatory techniques.

---

114. Van Alsenoy, *supra* note 111, at 9.

115. *See* Ryan Calo, *Against Notice Skepticism in Privacy (an Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1033 (2012).

116. Acquisti, *supra* note 45, at 6.

117. *Id.*

118. Solove, *supra* note 31, at 1880-81.

119. Acquisti & Grossklags, *supra* note 22, at 9.

120. Acquisti, *supra* note 45, at 6.

Behavioural insights help us understand and interpret these limitations and fallacies. Moreover, as recent research has shown, Behavioural Science, leveraging precisely on these cognitive limitations, can also effectively support policy-making in identifying appropriate mechanisms, e.g., nudging strategies, to help people's decision-making and, eventually, achieving privacy protection in practice.

Building upon the abovementioned interdisciplinary approach in the privacy field (integration of law and technology) a step further is proposed here: to learn the lessons from behavioural science[121] and to think of applying behavioural insights to policy-making in the area of *privacy*, in the wake of behavioural-informed regulation already operational in fields such as reduction of energy consumption, health care, consumer protection, etc.[122]

Cognitive psychology and behavioural economics, which provided meaningful insights on individuals' behaviour in many domains[123]—as discussed in the next part of this article—have recently also explained users' (apparently contradictory) attitudes and practices as regards their privacy protection.[124] Eventually, the privacy paradox receives clearer explanation (and possibly solutions) if looked in light of behavioural science.

What is suggested here is, in other words, to explore not only advanced technical versions of transparency mechanisms, but to identify and test alternative and complementary measures for users' better decision-making as regards data protection; a new approach that, without discarding the notice and choice system per se and taking into account behavioural insights, may provide more suitable, flexible and effective privacy-enhancing mechanisms, such as privacy nudges and "visceral notices," so called because based on certain common psychological reactions of individuals to design, instead of engaging the slower,

---

121. See, e.g., the research activities conducted by the Danish 'i-Nudge-you' team, INUDGEYOU, *available at* http://www.inudgeyou.com (last visited Dec. 20, 2015). On the increasing interest for behavioral science in policy and government management in USA, see also Courtney Subramanian, *'Nudge' Back in Fashion at White House*, TIME (Aug. 9, 2013), *available at* http://swampland.time.com/2013/08/09/nudge-back-in-fashion-at-white-house/ (last visited Dec. 20, 2015); Professor Kevin Werbach, Beyond Nudges: Gamification as Motivational Architecture, Speech at the 2013 CPDP Conference in Brussels (Jan. 23, 2013).

122. Michael S. Barr, Sendhil Mullainathan & Eldar Shafir, *Behaviorally Informed Regulation*, *in* BEHAVIORAL FOUNDATIONS OF PUBLIC POLICY 440, 444-45 (Eldar Shafir ed., 2012).

123. *See* Cass R. Sunstein, *Nudges.gov: Behavioral Economics and Regulation*, *in* OXFORD HANDBOOK OF BEHAVIORAL ECONOMICS AND THE LAW 719, 719 (Eyal Zamir & Doron Teichman eds., 2014).

124. *See* Acquisti & Grossklags, *supra* note 22.

reflective way of thinking: they show, rather than tell.[125]

The next part explores this line of research, after briefly considering challenges and opportunities of applying behavioural insights to policy-making in general. These strategies, alternative to traditional privacy notices might also represent a better implementation or at least integration mechanisms of the *Data Protection by Design* approach, as codified in the draft GDPR (Article 23).

IIII. INSIGHTS FROM BEHAVIOURAL ECONOMICS ON INFORMATION PROVISION

In this part, opportunities and challenges of behavioural sciences applied to public policy in general will be discussed, in order to better understand the relevance of behavioural insights in the *privacy* area.

A. *Applying behavioural science to policy: an overview*

Applied behavioural science, often referred to as Behavioural Economics ("BE"), studies human behaviour for better policy-making.

Since the 1970s, BE revealed that people, in their daily life, do not always act "rationally," as suggested by neoclassical assumptions in economics, making choices that lead to the best outcome for them: on the opposite, they often have preferences and take decisions that are not in their interests (suboptimal choices):[126] in other words, people are not perfectly rational in their cost-benefit considerations.

These deviations from rationality in individuals' decision-making are commonly referred to as biases (e.g., mental shortcuts or 'rules of thumb'), such as: *myopia* (people prefer short term gratifications to disadvantages in long terms); *social norms* (people are influenced by what the majority of people say or do, especially if there is a certain affinity with these people—compatriots or neighbours, etc.); *status quo* (people tend to stay with the default options); and *framing* or prime effect (people are influenced on *how* more than *what* information is given to them).

Such findings about human behaviour—very briefly recalled here—started to be taken into consideration by policymakers in the last decades and progressively incorporated in policy interventions focused on structuring the "choice architecture" for people's better decisions; the choice architecture is understood as the background against which decisions are made and that has major consequences for both decisions

125. *See* Groom & Calo, *supra* note 25.

126. *See* DANIEL KAHNEMAN, THINKING, FAST AND SLOW 12 (2011).

and outcomes.[127] Also, BE highlighted that this does not mean that people's behaviour is always irrational, random and unpredictable: on the contrary, it can be predicted, modeled and thus guided.[128]

BE has been regarded in recent years as a promising and exciting new development in public policymaking theory and practice.[129] Consequently, the efforts to bring more accurate understanding of human behaviour and choice to bear on law[130] have made that BE is now considered as the new paradigm for the study of choice behaviour and, on its basis, for the adoption of "behavioural informed regulation"[131] in the most different policy areas. The behaviourally-informed approach to regulatory problems, in fact, is gaining momentum, and its instruments, so called *nudges*, in the form of notices, warnings and default rules,[132] are becoming authentic policy tools.

The informal and cheap nature of these systems makes them more appealing as compared to traditional coercive regulatory mechanisms, like prohibitions, bans, etc. This regulatory approach is also called *libertarian paternalism*, because leveraging insights on individuals' attitudes and behaviours, claims to preserve their freedom of choice: the combination of paternalism and individual freedom would not be an oxymoron. This system is also named *soft paternalism* as opposed to hard paternalism.[133]

A number of public and private institutions have already embraced this approach as its instruments proved to be more effective than common legal instruments in addressing old and new challenges, like the energy consumptions reduction, health care, saving accounts, etc. In the U.S., the Obama Administration intensively counted on behavioural findings

---

127. Sunstein, *supra* note 123, at 1.

128. *See* Amitai Etzioni, *Behavioral Economics: Toward a New Paradigm*, 55 AM. BEHAV. SCIENTIST 1099, 1102-03 (2011); Mullainathan & Shafir, *supra* note 122, at 440.

129. *See generally* Ryan Bubb & Richard H. Pildes, *How Behavioral Economics Trims Its Sails and Why*, 127 HARV. L. REV. 1593 (2014), who, however, urge for greater awareness of the tension between the two "seductive" dimensions of Behavioural Law and Economics (its appeal as social science and politics) and consequent limits. Accordingly, policy-makers can in future resort to Behavioural economics for improving the design of law and policy (adopting choice-preserving regulatory tools) in more appropriate and context-dependent ways, *i.e.* pondering advantages and disadvantages of the different regulatory mechanisms (traditional or new) available.

130. *See* BEHAVIORAL LAW AND ECONOMICS 1 (Cass R. Sunstein ed., 2000).

131. *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).; Mullainathan & Shafir, *supra* note 122, at 428.

132. THALER & SUNSTEIN, *supra* note 131.

133. *See* Oren Bar-Grill, *Consumer Transactions*, *in* THE OXFORD HANDBOOK OF BEHAVIORAL ECONOMICS AND THE LAW 465, 478 (Eyal Zamir & Doron Teichman eds., 2014).

for a number of initiatives and in UK an ad hoc 'Behavioural Insights team' within the Cabinet office has been created.[134] At the intersection of "applied behavioural science, public institutions, NGO's and private stakeholders" are initiatives such as *iNudgeYou* - initiated as a Danish Nudging Network and become an international landmark.[135]

European policy-making is also increasingly relying on behavioural insights, both at its design and its implementation phases. Surveys to collect consumers' perceptions and preferences, lab experiments and more accurate behavioural observation methods (i.e., *randomized controlled trials*) are promoted by the EU in different areas of intervention, with the aim to foster better individuals' decision-making.[136] Behavioural insights are, for instance, at the basis of the recent regulation aimed to limit the default options in consumer contracts or to improve consumer protection in booking travel packages.[137] As a new but quite spread trend, varying communitarian goals are being pursued through nudging strategies such as "green behaviors,"[138] as well as improvement in consumer decisions regarding, for instance, retail investments[139] or, more recently, digital purchases.[140]

B. *Applying behavioural science to policy: challenges and*

134. *See Who We Are*, BEHAVIOURAL INSIGHTS TEAM, *available at* http://www.behaviouralinsights.co.uk/about-us/ (last visited Dec. 20, 2015).

135. *See iNudgeyou – The Danish Nudge Unit*, iNUDGEYOU, *available at* http://inudgeyou.com/about-us/ (last visited Dec. 20, 2015).

136. *See generally* Rene van Bavel et al., *Applying Behavioural Sciences to EU Policy-Making*, JRC SCIENTIFIC AND POLICY REPORTS EUR 26033 EN 14-19 (2013), *available at* http://ec.europa.eu/dgs/health_consumer/information_sources/docs/30092013_jrc_scientific_policy_report_en.pdf (last visited Dec. 20, 2015).

137. *See* Council Directive 2011/83, art. 22, 2011 O.J. (L 304) 64, 81 (EU); *see also Commission Proposal for a Directive of the European Parliament and of the Council On Package Travel and Assisted Travel Arrangements*, at 4, COM (2013) 512 final (Sept. 7, 2013).

138. *See, e.g.*, *Science for Environmental Policy Future Brief: Green Behaviour*, EUR. COMMISSION (Oct. 2012), *available at* http://ec.europa.eu/environment/integration/research/newsalert/future_briefs.htm (last visited Dec. 20, 2015).

139. *See, e.g.*, *Consumer Decision-Making in Retail Investment Services: A Behavioural Economics Perspective* (Nov. 2010), *available at* http://ec.europa.eu/consumers/archive/strategy/docs/final_report_en.pdf (last visited Dec. 20, 2015).

140. *See, e.g.*, Gabriele Esposito, *Consumer Information in the Digital Online Market – A Behavioral Approach*, CIDOM REP., JRC SCIENTIFIC & TECHNICAL REP. 5, *available at* http://ec.europa.eu/justice/consumer-marketing/files/report_cidom_final.pdf (last visited Dec. 20, 2015).

opportunities

As said before, policy-making is increasingly relying on behavioural studies and nudging strategies for citizens' better decision-making in different areas of intervention.

This happens, however, not without concerns.[141] Applying behavioural science to policy-making requires a thorough consideration of a number of different issues.[142] At least two main categories of problems can be identified as far as the application of the behavioural approach to policy-making is concerned. On the one hand, the legal grounds of its mechanisms that rely on influence and persuasion in order to obtain a behaviour change and creates a new power, potentially subject to abuse. On the other, their (lack of) generalized applicability: a nudge might not have the expected outcome if used in different areas or with different audiences.

The same legitimacy of the nudging system itself within a democratic society might be put in doubt or at least questioned.[143] Most existing criticisms seem to point to the fact that, while a good nudge influences individual choices without changing freedom of choice, sometimes the line between persuasion and manipulation is not easy to see and goes together with the fear of being maneuvered.

Nudges can be stronger or weaker than the law and coercive as well, but the problem is the risk that they might be adopted without the legal safeguards proper of the legislative processes. Moreover the effect of nudges may be very different, depending on context or on the interests of the parties involved.[144]

A substantial regulation of these alternative measures is, therefore, urged, capable to formalize these behavioural-informed mechanisms and

---

141. *See, e.g.*, Karen Yeung, *Nudge as Fudge*, 75 MODERN L. REV. 122, 123-24 (2012); *see also* Alberto Alemanno & Alessandro Spina, *Nudging Legally. On the Checks and Balances of Behavioural Regulation*, 12 INT'L J. CONST. L. 429 (2014).

142. Neven Mimica, *Applying Behavioural Insights to Policy-Making: Results, Promises and Limitations* (Sept. 30, 2013), *available at* http://ec.europa.eu/dgs/health_consumer/information_sources/consumer_affairs_events_en.htm (last visited Dec. 20, 2015) (discussing the opportunities and limitations of applying behavioral science to policy making in all areas of interest at a European Commission conference in Brussels).

143. *See* Pelle G. Hansen & Andreas M. Jespersen, *Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy*, 4 EUR. J. RISK REG. 3, 5 (2013); Alemanno & Spina, *supra* note 141, at 445. *See generally* Anne van Aaken, *Judge the Nudge: In Search of the Legal Limits of Paternalistic Nudging in the EU*, *in* NUDGE AND THE LAW: A EUROPEAN PERSPECTIVE 83 (Alberto Alemanno & Anne-Lise Sibony eds., 2015).

144. *See generally* Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155 (2013).

to guarantee an oversight system of the new kind of power they bring with.[145] Notwithstanding their informal nature, and given their persuasive quality, the adoption of these mechanisms cannot circumvent basic principles of the State of Law, such as legality and impartiality. An appropriate oversight system on behavioural-informed tools can guarantee a smooth integration of behavioural science into public policy. As some scholars propose:

> [A] general requirement imposed to public administrations to systematically consider formalized behavioral mechanisms at the pre-legislative stage could serve to accommodate in a more principled and consistent way these insights into policy making while at the same time protecting them from possible abuses.[146]

Their enclosure within the framework of essential legal principles like *proportionality* seems necessary. These behavioural-based measures should be pondered according to minimum criteria: their capacity of pursuing a legitimate goal (i.e., individual, societal welfare); their suitability; necessity (other available measures are not effective); proportionality *stricto sensu* (i.e., the mildest measure have been chosen); and foreseeability (at least as regards their purposes and consequences). Invisible, non-transparent nudges should be considered not admissible.[147]

A concrete guideline for policy-makers in order to avoid the adoption of tools of illegitimate manipulation of people's choice, may be the distinction between *transparent and non-transparent* nudges, which might help to distinguish the manipulative use of nudges from other kinds of uses and therefore to adopt a more responsible use of nudging approach to behavioural change.[148] In particular, the choice of policy-makers should fall on nudges aimed at promoting decision-making in ways that are *transparent* to the people influenced, by "making features, actions, preferences, and/or consequences salient, or by providing feedback . . . ."[149] This kind of interpreting and guiding frameworks for the use of 'nudges for good' should be endorsed so that nudges, if chosen and adopted as policy tools, can work at the service of libertarian paternalism.[150]

Another aspect that should be borne in mind, is that alternative, non-traditional methods of changing citizens' behaviour, whether they are

145. *See generally id.* at 1229.
146. Alemanno & Spina, *supra* note 141, at 455.
147. van Aaken, *supra* note 143, at 29-33.
148. Hansen & Jespersen, *supra* note 143, at 23.
149. *Id.* at 24.
150. *See generally* THALER & SUNSTEIN, *supra* note 131, at 5-6.

classified as *code* (like in the techno-regulation), *nudges*, or *notice* (information disclosure), may both facilitate (*help*) or hinder (*friction*) decision-making and a certain conduct.[151]

Some non-traditional public interventions, if focused on obstacles or barriers, may be more coercive than the law; physical barriers or digital ones (*code*) like Digital Right Management Systems ("DRM") to enhance copyrights, but also psychological ones, like some new virtual speed limits made of painted images on the road (*nudges*) introduce an obstacle to a conduct, making it harder or impossible for the individual to act differently. In this case, resisting to a nudge is not without costs, like discomfort, time associated to overcoming the architecture of the choice; the individual autonomy in these cases might be unreasonably jeopardized. In other words, the problem with these alternative measures based on *friction*, would consist in the fact that they may introduce costs and burdens to citizens while, meantime, they may be adopted without the legal safeguards and guarantees proper of the legislative processes, i.e., to be discussed, voted on by elected representatives and in cases, challenged.

However, as Calo stresses, alternative mechanisms for behavioural changes do not necessary and always need to build upon friction, like they do some technical barriers to replace the deterrence function of law (e.g., the doors accessing to a metro station, or the DRMs for copyright protection, or the digital filters installed on a computer for the safety of children).[152] Alternative systems should work by helping, nudging, citizens to arrive to their own goals; instead of studying human behaviour and cognitive biases in order to contrast them, it is better to help them. An example may be represented by placing fruits or other healthy food at eye-level in the cafeteria of a working place.

If policy intervention aims at modifying the choice architecture, altering physical or digital environment, this should be not to impede, prevent certain conducts but to facilitate better decision-making: "the technology should keep its capacity to enhance and not diminish certain essential democratic processes."[153] Accordingly, regulators should explore the possibilities for helping citizens (in using code, nudge or notice mechanisms—or a combination of them) in achieving by themselves their own goals, before introducing forms of alternative but coercive mechanisms (which may lack the safeguards and the process of the law).

---

151. Calo, *supra* note 108, at 777.

152. *Id.*

153. *Id.* at 798.

Therefore, when deciding about changes in architecture, regulators' preference should be, where possible, for *facilitation* not for imposing barriers, according to the theory that "we should abandon the safeguards that [support the] law only when it can be said that we are helping citizens do what they would do if they had the right information and tools."[154]

As Calo stresses, combining certain elements of different strategies provides more possibilities for facilitation.[155] A traditional *notice* does not work, but elements of *code* and *nudge* may improve notices so to become more effective, especially when notices are provided at the point of decision-making and this is particularly relevant in the field of privacy and data protection, as discussed below.

An example of successful notice mechanism relying on "nudging" is offered by initiatives seeking to curb obesity, which instead of focusing on traditional notice mechanisms like caloric information labels to ameliorate people's eating/drinking habits, show the physical activity equivalent needed to burn a certain amount of calories, e.g., running, biking, etc.,[156] or seek to directly encourage people to do more exercise.[157]

This facilitation role is not an easy task either; it is difficult to understand when and how to facilitate decision-making (and to renounce it because it does not work). Decision-making can depend entirely on the framing or on the context, but in doubt of what influences our preferences, we should adopt, as a guiding principle, *facilitation* rather than *friction*.[158] At the end of the day, it is not important how we label a public intervention in the choice-architecture as *code*, *notice or nudge*, but regulators should look at the interventions that help. This can mitigate also the concerns mentioned before about the legitimacy of nudging strategies.

C. *Applying behavioural science to policy: from information overload to smart disclosure in Consumer Protection and in Data Protection*

As demonstrated in other sectors (marketing or organization science), the excess of information may have a negative effect on users' choice quality.[159]

---

154. *Id.* at 800.

155. *Id.*

156. Sara N. Bleich et al., *Reduction in Purchases of Sugar-Sweetened Beverages Among Low-Income Black Adolescents After Exposure to Caloric Information*, 102 AM. J. PUB. HEALTH 329 (2012).

157. Amitai Etzioni, *On Curbing Obesity*, 51 SOC'Y 115 (2014).

158. *See* Calo, *supra* note 108.

159. *See generally* Byung-Kwan Lee & Wei-Na Lee, *The Effect of Information*

Insights from behavioural studies have shown, in fact, that even when presented with full information, consumers may not always be able to understand or use information in their interest, i.e., to make the best choice. This can be due to not necessarily the lack of information, but to the fact that most of the information is not good; moreover, too much information (although correct and accurate) may be useless and even harmful. There is a moment in the information acquisition (like for the information that we receive when we decide to buy a product or service) in which the cost that a consumer has to spend to process the information is higher than the benefit of ignoring it: this is also called "information overload."[160]

Studies on information overload and its effects on consumer decision-making suggest that what matters is not (necessarily) to provide the consumer with *more* information but to provide her with the *good* one.[161]

This is particularly relevant in the digital environment, on the Internet, where users are constantly exposed to tons of information difficult or impossible to absorb, to interpret and to use. The problem with the traditional information notices (including privacy notices) is that they constitute in many cases an example of "information overload." Burdening the individual with information (whether it is on products and services or on how personal data is processed or protected), is not the solution.

As said before, one of the main lessons that policy-makers receive from behavioural scientists is to work on the *choice architecture*, the social background against which consumer decisions are made.[162] In this way policy-makers are called to become a sort of choice architects, able to make the appropriate, small changes in the underlying environment that may have a large impact on people's behaviour. "Such changes may involve disclosure, warnings, default rules, increased salience, and use of social norms."[163]

Overload on Consumer Choice Quality in an On-Line Environment, 21 PSYCHOL. & MARKETING 159 (2004).

160. *Id.* at 177-78.

161. See the example of the regulatory measure adopted in US to counter the level of obesity and imposing requirements to indicate the calories information on restaurant menus, which did not get the expected results as people ignored them. Brian Elbel et al., *Calorie Labeling, Fast Food Purchasing and Restaurant Visits*, 21 OBESITY 2172 (2013).

162. THALER & SUNSTEIN, *supra* note 131.

163. Cass R. Sunstein, *Behavioral Economics, Consumption, and Environmental Protection* 1 (Harvard Kennedy Sch. Regulatory Policy Program, Working Paper No. RPP-2013-19, 2013).

The most important modification that should be made is *salience*:[164] salience of certain product's features or of a situation (like prices, sizes, incentives), and, above all, of the information to be provided to people about these features. Salience can work, in fact, as a *nudge*.[165] Therefore, the information that people receive should be *salient*, upon *salient* features and provided in a moment and a situation *salient* for these people, enabling a process of "smart disclosure," i.e., of a more effective information provision by those who are responsible for - that the public policy is called to encourage.

Behavioural studies have invalidated a typical assumption underlying many of the current public policies in consumer protection, i.e., that individuals would make a cognitive effort to weigh costs and benefits before taking a decision like buying or not buying a product. In this way, they not only have shown that biases are also typical of policy-makers (as made of human beings), but building upon Kahneman's insights about human cognitive processes,[166] have also highlighted that people predominantly use the *fast thinking* system, that is, more intuitive, more instinctive and rapid way of making decisions.[167]

This suggests that traditional information policies are disregarding important components of human cognitive process that reflect into consumers' behaviour and that this might be the reason of their failure to realize societal and individual best interests. This raised the question whether a different, innovative policy intervention might be necessary to help consumers adopt decisions in their best interests.[168]

An important finding of BE (which has also shown to be useful in order to attain a better public policy by conducting ad hoc experiments) is that the more our activities are routinized, repeated on a daily basis, the more we employ the *fast thinking* system. This is particularly interesting for the decisions we take every day with regards to digital activities (electronic communications, e-transactions, access to a service or product); our activities on the Internet (and on the mobile digital applications) are often made of repetitive and systematic gestures: clicking a button while visiting websites, downloading applications or

164. *Id.* at 6, 9, 15-16.

165. Sunstein, *supra* note 123, at 721.

166. Kahneman, in particular, makes the distinction between *thinking fast* and *thinking slow*, and, as a consequence, between automatic behaviours and reflective choices. *See* KAHNEMAN, *supra* note 126.

167. *Id.*

168. Org. for Econ. Co-operation and Dev. [OECD], *Enhancing Competition in Telecommunications: Protecting and Empowering Consumers*, at 39, OECD Doc. DSTI/ICCP/CISP(2007)1/FINAL (May 24, 2008).

documents, sharing thoughts or pictures, etc. This is particularly true with regard to terms and conditions of an online contract, that, in most of the cases, we accept without reading them, as well as with regard to *privacy policies*.

In light of recent specialized studies on users' privacy attitudes and preferences, in fact, what was just observed for consumer information seems to be valid for information privacy and related users' behaviour.[169] Consumer Protection (strictu sensu) and Data Protection are two interconnected (though distinct) areas.[170] First, because the two fields correspond to two very close EU law domains; the status of data subject and of online consumer are often aligned or overlapping, with the data subject being very often *also*, *in the meantime*, a consumer; secondly, because the information provision obligation (bearing on data controller or on service provider, who may coincide) and its effects on the corresponding individual's decision-making has equivalent relevance (in one case, regarding his consumer behaviour in buying a product/service, in the other one his citizens' behaviour in disclosing (or not) personal data).

Given the extraordinary growth of Internet services and online transactions, Data Protection is becoming increasingly important for consumer.[171] The attention for it, therefore, is increasing, as it may represent one of the instruments to realize the *consumer protection.*[172] In other words, data protection is also (and in addition to its independent status of a fundamental right) a way to attain consumer protection, especially online; thus, similarities in the assessment of legal and non-legal tools employed to strengthen individuals protection in the two fields, namely information notices and *nudges*, may be drawn.

Recently, policy-makers started to work on minimizing detriment to the consumer's interest resulting not only from a lack of information or misleading information regarding services and products, but also from

169. *See* Acquisti & Grossklags, *supra* note 22.

170. *See* IRIS BENOHR, EU CONSUMER LAW AND HUMAN RIGHTS 166 (2013).

171. *Id.* at 59.

172. The consumer protection has a principle status in the Charter of Fundamental Right of the EU (Article 38), in the sense that it is intended as a legal principle rather than to have the status of a subjective right. However, as other legal principles, this provision in the Charter could evolve in the future and become a right (maybe with the development of the case law). In particular it may become more concrete if it applied in combination with other rights of the Charter. *Id.* (demonstrating that it is already happening). Article 38 could be applied in combination with other rights of the Charter or constitutional provisions, for instance with Article 8 on the right to data protection "in fact in some national cases a cumulative application of basic provisions has resulted in successful claims for individuals." *Id.* at 64.

the "bounded rationality" of consumer decision-making.[173] If the individual, recipient of the disclosure, is overwhelmed by information without the possibility to discern what information is important, then disclosure will have little positive effect. Behavioural studies have demonstrated that alternative ways that try to *induce* people to behave in their best interests may work better than traditional notice and choice or "command and control" measures.[174] Regulators can learn how to enhance information disclosure's effectiveness: "Disclosure has many limitations, but there is also great opportunity for enhancing its beneficial effects."[175]

Consumer protection passes also by competition enhancing policies[176] that focus their attention on *demand* side analysis (i.e., based on insights from consumers' behaviour analysis). Policymakers and regulators started to consider the needs and motivations underlying consumer behaviour in communication markets, while in the meantime, raising awareness about possible risks for consumers as well as opportunities of protection. A main instrument to improve consumer protection (and satisfaction) online has been identified in the quality of information provision. New requirements have been introduced compelling, for instance, all major service operators to provide complete, comparable and accurate information to consumers to reduce the "information asymmetry" between operator and consumer and to enable the latter to take the most suitable choices among products and services offered online and therefore, among providers.[177]

Likewise, we assisted to a proliferation of information obligations and accountability rules in the Data Protection law, also in view of ensuring a fair development of the digital single market, increasingly an

---

173. *Id.* at 81-82.

174. *See Applying Behavioural Insights to Reduce Fraud*, U.K. CABINET OFF. BEHAVIOURAL INSIGHTS TEAM (2012), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60539/BIT_FraudErrorDebt_accessible.pdf (last visited Dec. 20, 2015).

175. Sunita Sah, Daylian M. Cain & George Loewenstein, *Confessing One's Sins But Still Committing Them: Transparency and the Failure of Disclosure*, *in* BEHAVIOURAL PUBLIC POLICY 148, 158 (Adam Oliver ed., 2013).

176. OECD, *supra* note 168, at 5.

177. The idea is that further developments in competition policy should serve the consumer interest. *See id.* at 6. The purpose of pro-competition policy is to enhance consumer welfare; in other words, consumer protection and empowerment should be based on pro-competition policy and mechanisms that have the consumer interest as priority. *Id.* at 4 ("[W]here consumers have little information or poor quality information . . . they may end up misled and confused by the choices on offer, may pay too much or buy the wrong service. This may, in turn, inhibit and dampen the competitive process. . . . [Consumers] need to be able to move quickly and with the minimum constraint between service providers.").

information-rich market. Providing innovative and more effective information mechanisms for privacy may also prove to be an innovative and effective competition-enhancing tool, which may benefit individuals as well as businesses and the market in general.

Insights from BE, in fact, recently proved to be helpful also to explain the privacy paradox (i.e., even in the presence of privacy notices and warnings,[178] users tend to disclose a large amount of data) and to find more effective privacy-enhancing mechanisms.

A multitude of systematic deviations from rational decision-making that seems to have an impact on users' *privacy decisions-making*, besides "incomplete information" and a "bounded cognitive ability" to process the available information (information asymmetry and transactional costs), has been identified.[179] These deviations can be explained through the same cognitive biases that BE has revealed in other areas: individuals cannot see the risks deriving in the future from their data disclosure (or from the use of a service that implies automatic data collection) and go for immediate gratification of, for instance, free service (*myopia*); users tend to stick with default options, this highlights the relevance of default privacy settings for the privacy online; few users change them in practice (*status quo*); users' privacy behaviour seems to be more influenced by an image or an alert than by a long, though comprehensive, text (*framing* effect).

Several behavioural biases, therefore, come into play and are critical for the effectiveness of privacy policies. Like the legal information notices on products and services relevant in consumer transactions, privacy policies "are important transparency mechanisms, but are not likely to be decisive in determining user behavior. . . . [They] are [not] salient to consumers . . . ."[180] Although these reflections on privacy policies are related to consumer's behaviour in the context of online transactions, they are seemingly applicable to users' privacy behaviour in

178. A clarification is needed. The concepts of information notices and warning messages may be (legally and technically) distinct and may have different purposes that should be taken into account when testing and assessing users' willingness to disclose data: basically, the first have the purpose to inform about what/how data are collected and protected, about users' rights, about the identity of the data controller, etc., while the warning messages work as caveats, admonitions about possible risks of data disclosure: privacy policies may contain both type of information, but, generally, current polices are made predominantly of the first type.

179. Acquisti & Grossklags, *supra* note 22, at 364.

180. *See* Irion & Luchetta, *supra* note 30, at 36-37, where it is argued that only if privacy choices are embedded in a given transaction and effectuated by rules surrounding the sign-up are consumers likely to align with their privacy preferences: "Hence, opt-in and opt-out rules as well as default settings have strong impacts on the level of data disclosure."

general, when facing information provisions.

There is a need for making the access to privacy policies easier, simpler, agile and therefore more effective, so that users may be able to make more informed decisions regarding the (direct or indirect) disclosure of their personal information online.[181]

IV. TOWARDS REGULATED PRIVACY NUDGES?

Knowing how users really behave with regard to their personal data (often in contrast with their statements) may play a relevant role in addressing the gap between existing legal privacy safeguards and implementing tools. Therefore, like for other areas of policy intervention, a better understanding of data subjects' behaviour should be of interest for policymakers as it can assist them to design better privacy policies and, ultimately, to fill in this gap; behavioural insights can be applied so to identify and adopt innovative privacy-protecting measures.

The solution to the privacy paradox, in fact, does not seem to be the introduction of new principles and rules. Behavioural economics propose the introduction of (tested) tools like "privacy nudges" to be applied in contexts of behavioural advertising, location sharing and social networks.[182] More suitable, effective privacy tools, capable to keep pace with modern times, but especially to support users in their decision-making, i.e., "supporting-choice mechanisms,"[183] should be introduced.

As said in the previous part, behavioural science applied to policy-making is not new to European institutions, as a number of experimental studies in support of policy initiatives are being run by the European Commission. Still, the consideration of behavioural insights in the specific area of *privacy* is very limited in Europe, both at academic and institutional levels and restricted to the analysis of behavioural patterns in online users as regards their data disclosure habits.

Few experimental studies have been commenced in the EU, as discussed below. However, there hasn't been so far, to my knowledge, any completed experimental study in Europe testing the nudging effects on users' behaviour, as a way to foster a privacy-protective behaviour, nor the application of behavioural science to policy-making in the area of *privacy*. Also in Europe, we should support the idea that, instead of discarding the option of notice and choice (i.e., informed consent),

181. *See generally* Acquisiti & Grossklags, *supra* note 22.

182. Alessandro Acquisti, *From the Economics to the Behavioral Economics of Privacy: A Note*, *in* ETHICS AND POLICY OF BIOMETRICS 23, 23-26 (Ajay Kumar & David Zhang eds., 2010).

183. van Aaken, *supra* note 143, § III, § C.

because it is not effective, it is worthy to try improving it with *nudging mechanisms*, which help citizens to make their decisions on data protection/disclosure, i.e., using appropriate behaviour insights to create more effective *privacy notices*.

Privacy nudges, as complementary regulatory tools would seek at encouraging, at *nudging* a privacy-protective behaviour, while preserving the freedom of choice of the users, achieving the *soft* or libertarian paternalism: as said before, it is not an *oxymoron*, if well interpreted and implemented.[184] There seems to be enough space for its application also in the *privacy* area.

Nudging privacy seems to be possible and desirable, once the conditions for its application (similar to those applicable to other areas) are satisfied, i.e.: (1) the privacy nudges are subject to an oversight mechanism and proportionality test; (2) given that these mechanisms may have a double side quality (i.e., preserving and compromising freedom at the same time), avoid that users are heavily charged with the responsibility of DP; (3) the privacy nudges have been proven to work—i.e., to have a positive impact on a target, being it privacy-preserving behaviour or increased awareness; and (4) ensure control mechanisms of companies compliance with DP obligations, the latter point may entail strengthening the powers of national DP authorities. Further research may investigate the best and efficient way to identify and implement these control mechanisms.

Soft paternalism and nudging strategies, under these conditions, can be the way forward for privacy protection online.

A. *Visceral notices*

Against this background, and without dismissing a rights-based approach, perhaps it is time also in Europe to build upon that strand of international lawyers and behavioural scientists who have proposed a new dimension of privacy notices as innovative strategies that impact privacy-related attitudes, like the so-called "visceral notices."[185] The main underlying idea is that information notices should have less text and more interaction.

Unlike traditional notice that relies upon text or symbols to convey information, "emerging strategies of 'visceral' notice leverage a consumer's very experience of a product or service to warn or inform."[186] Moreover, they prove to be useful tools to better inform users about data

184. Sunstein, *supra* note 163, at 313-27.

185. *See* Groom & Calo, *supra* note 25, at 3.

186. Calo, *supra* note 115, at 1027.

collection practices (i.e., hidden collection).

Some visceral notices are particularly interesting because based on "certain common psychological reactions to design to change a consumer's mental model of a product or service; and 'showing' consumers instead of 'telling' them, i.e., demonstrating the result of company practices for the specific consumer, rather than describing the practices themselves."[187]

Previous experiments[188] not only demonstrated the weakness of traditional explicit notices, but also that *visceral* notices are more successful at eliciting privacy-protective behaviour, by pulling users' automatic responses.[189] Visceral notices, such as an interactive character that speaks or moves her eyes while user types or moves the mouse, or the display of the user's location or browsing history, seem to affect privacy-related attitudes and behaviours.

Not every nudge has the same effect and is interchangeable, though. A relevant finding of these studies is that a visceral notice represented by an informal interface ("informal condition") to be employed, for instance, in children's websites, prove to reduce privacy concerns, *but also* to increase data disclosure by users, making the informal design problematic for data protection and privacy policy.

User data disclosure is a complex behaviour.[190] People disclose their information also indirectly, that is, when they are not asked (directly) to reveal their data, when they are not alerted to the sensitivity of the information itself and therefore not urged to "regulate" the disclosure of information. In the indirect disclosure (very frequent in Web browsing), the traditional notice mechanism clearly fails its goal:

> The drive to regulate does not minimize passive [i.e., indirect] disclosure. Passive disclosure is more successfully minimized with visceral notice strategies, such as interactive agents, because they directly affect the desire to disclose and do not rely on the more thoughtful process of determining if privacy is threatened.[191]

The use of a visceral notice such as an interactive agent (e.g., an anthropomorphic silhouette), minimizes user's data disclosure, without relying on service provider's privacy policy. In other words, it appears that this kind of visceral notice has better impact on the user's "fast thinking."

---

187. *Id.* at 1033-34.
188. *Id.* at 1054.
189. *See* Groom & Calo, *supra* note 25, at 27.
190. *Id.*
191. *Id.* at 28.

Most important, this sort of *nudge* seems to succeed in eliciting privacy-protective behaviour, reducing data disclosure without creating privacy concerns (what traditional transparency tools usually do).

1. *The BREVE experimental project: Behavioural Responses to Privacy Visceral Notices*

Building upon previous research on "visceral notices"[192] and on "privacy nudges,"[193] the project *Behavioural Responses to Privacy Visceral Notices* ("BREVE") has been undertaken by one of the research institutes of the European Commission between 2013 and 2014.[194]

This study examines, via an online experiment and a survey, how users' online behaviour changes when they are exposed to visceral notices[195] and real-time alerts about the data collection practices associated with their online activities.[196] The underlying idea is to assert to what extent the use of well-designed, intuitive notices effectively change users' behaviour as regard personal data disclosure.[197] The goal

192. *Id.*

193. Yang Wang et al., *Privacy Nudges for Social Media: An Exploratory Facebook Study*, PROC. OF THE 22 INT'L CONF. WWW COMPANION (2013). *See generally* Leslie K. John et al., The Best of Strangers: Context Dependent Willingness to Divulge Personal Information (July 6, 2009), *available at* http://ssrn.com/abstract=1430482 (last visited Dec. 20, 2015); Lior J. Strahilevitz, *Privacy and Technology: Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010 (2013); Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE SECURITY & PRIVACY 82, 82, 84 (2009); Alessandro Acquisti et al., *The Impact of Relative Standards on the Propensity to Disclose*, 49 J. MARKETING RES. 160 (2012).

194. *Behavioral Economics*, JOINT RES. CENTRE, *available at* http://is.jrc.ec.europa.eu/pages/BE/BEindex.html (last visited Dec. 20, 2015) (for more information about the BREVE project).

195. Groom & Calo, *supra* note 25, at 27.

196. In particular, a series of online experiments on EU users, in which 8 conditions, represented by different privacy notices, is run: beside the traditional (standard and simplified text notices), five types of more innovative notices are displayed to different groups of online participants, who were asked to assess a new (mock-up) search engine, in particular: an anthropomorphic agent (static and interactive); the IP and the search history (displayed on a side of the screen); an informal interface (colourful and youngish appearance). Wang, *supra* note 193.

197. The online experiment involves, in the first phase, the construction of a mock-up search engine that the participants are invited to evaluate through a survey; in the second part, participants are asked to choose among some trivial questions and search for their answers through the search engine: in this phase, the choice of the questions is what matters most. Since these questions vary in terms of the nature and amount of personal information they lead participants to reveal, the choice of questions by participants represents a measure of their level of indirect disclosure of personal information. In fact, one of the three questions in each set (randomly) is a personal data-disclosure question (such as: "What is the street address of a post office in the town where you live?"). The differences among treatments is given by the presentation of different privacy notices (including visceral notices), that are

is to check if any of the treatments affects participants' privacy concerns, if it leads to a significant different personal data disclosure (both direct or indirect data disclosure) and what policy considerations can be drawn.[198]

B. *Integrating behavioural insights into privacy policy making?*

Once the issues on legitimacy of innovative privacy notices (namely visceral notices or privacy nudges) are addressed and after having tested their effectiveness in changing users' behaviours via ad hoc, reliable experiments, the attention should then turn to consider when and how to integrate these mechanisms into policy-making (and into real life).

Behavioural science can be applied to public policies whenever there is a behavioural element to them. It can help design new policies, suggest improvements to existing ones, or provide ex-post explanations of why the target group of a specific policy reacted in a particular way.[199]

When considering at what stages of policy-making behavioural insights and its strategies should be introduced,[200] behavioural aspects should be incorporated (at least) in the following phases of *privacy* policy-making:

First of all, at the first stage of the policy design, where policy-makers seek to understand users' behaviour surveys on online users' practices as regards their personal data (e.g., biases explaining privacy paradox) have been run in several countries as mentioned before and also in the EU; an example is given in the Special Eurobarometer 359/11 and related report published by the Eurpoean Commission ("EC") in 2011.[201] Other specific studies are not missing in Europe, like the one on privacy-friendly default settings, carried out within the SPION project.[202]

However, in order to test the responses of users to innovative privacy strategies, field trails, from which policy recommendations may be drawn, are needed—like those started to be run in the U.S. on privacy

---

expected to (differently) impact users' disclosive behaviour. *Id.*

198. At the time of writing, the BREVE experiment is underway: results of which are expected to be published soon.

199. *See* Rene van Bavel et al., *supra* note 136.

200. *Id.*; *see also* Alemanno & Spina, *supra* note 141.

201. *See Pan-European Survey of Practices*, *supra* note 18, at 6.

202. *See generally* Alessandro Acquisti & Fred Stutzman, *Behavioral Aspects of Privacy in Online Social Networks*, SPION (Dec. 21, 2012), *available at* http://www.spion.me/workpackage/behavioral-aspects-of-privacy-in-online-social-networks (last visited Dec. 20, 2015).

nudges[203] and visceral notices.[204] These responses are still not enough explored in Europe and studies like BREVE (where a series of different privacy notices are tested on EU users) are exceptional.[205]

Still at the policy design stage, behavioural insights may be employed in the context of the Impact Assessment ("IA"), as one of the pillars of the EC better regulation strategy in different areas of policy intervention.[206] The IA document accompanying the EC Proposal for a GDPR makes some reference to behavioural research; however, more could be done at this level.

As Alemanno & Spina notice, "behavioural considerations may allow policy makers to not only consider a broader set of regulatory options and test their effectiveness through Randomized Controlled Trials ("RCTs"), but also to empower citizens to have a say thus increasing the accountability of the regulatory outcome."[207] These considerations should include testing the policy options (via in field experiments).

Secondly, at the formal stage of law-making process, transferring behavioural considerations into primary or secondary law. At this step, several issues should be considered in future research, such as: should the law impose stricter requirements for online privacy policies, to be 'visceral' and effective[208] (e.g., requirements related to the website architectural design or also on the pursued behavioural change effect)?; How detailed should the privacy law be in this regard?; Would the introduction of specific legal requirements for effective privacy policies, like visceral notices, be feasible and affordable for industry and consumers?; and Would the visceral privacy notices be better introduced with soft law instruments (e.g., recommendations), in which evidence-based models of privacy measures might be strongly urged to industry?

Third, at the implementation level:

---

203. *See* Acquisti, *supra* note 182, at 24-25.

204. *See* Groom & Calo, *supra* note 25, at 15.

205. Needless to say that experiments of this kind on users' behaviour should be conducted in compliance with legal and ethical principles, starting from informing the participants about the purposes of the tests (at least about the general goals and before using their data). Principles seem to not have been followed by some social networks in their recent practices. For example, for a week, Facebook members were unwitting participants of an experiment in direct emotional manipulation. Alex Wilhelm, *Facebook and the Ethics of User Manipulation*, TECHCRUNCH (June 29, 2014), *available at* http://techcrunch.com/2014/06/29/facebook-and-the-ethics-of-user-manipulation/ (last visited Dec. 20, 2015).

206. *Impact Assessment Guidelines*, at 4, SEC (2009) 92 final (Jan. 15, 2009).

207. Alemanno & Spina, *supra* note 141, at 456.

208. *See* Calo, *supra* note 115, at 1071-72.

It would be possible to introduce more innovative privacy notices through implementing acts of supranational or national legislation, like implementing acts of the European Commission or European guidelines. Some good examples already exist but are limited to better information provisions.[209]

Another possible integration of behavioural insights at this level might be within the specific *Data Protection Impact Assessment* that any controller will be required to run according to the Draft GDPR, when "processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes" (Article 33).[210] The use of behavioural insights might be very useful, as it would allow to better assess the impact of risky technologies on users' privacy and their perceptions, as well as the effectiveness of privacy-protecting measures to be adopted by the data controller.

However, this would not be painless. Several issues are at stake. Should behavioural considerations be *imposed* by law at this stage? Furthermore, should, for instance, an ISP conduct his own evaluation about how the application of privacy nudges on his website may reduce risks for privacy, impacting on users' behaviour and should he decide which nudge is more appropriate? Economic considerations may bring him to choose the less appropriate nudge; although a very informal, youngish interface may be of negative effect on users' protective behaviour, it might increase trust in his website and, consequently, increase personal data disclosure (necessary for its business model).[211]

A DP assessment, if any, might be made at a higher level, e.g., by the EDPS, the European DP Supervisor, or by the national Data Protection Authorities and for categories of data controllers (e.g., ISPs). In this case, visceral notices or other kinds of privacy nudges may represent valuable options that add to a wider framework of requirements aimed at obtaining a sort of data protection certification, like privacy seals,[212] which are encouraged by the Draft GDPR (Article 39).

---

209. *See* Luzak, *supra* note 83, at 549. See also Exec. Order No. 13563, 3 C.F.R. 13563 (2011), which promotes increased public participation throughout all stages of the rulemaking process and encourages public agencies to consider regulatory approaches such as default rules, disclosure, and simplification that nudge citizens toward better choices while allowing them to retain flexibility and liberty of choice.

210. Artemi R. Lombarte, *The Madrid Resolution and Prospects for Transnational PIAs*, *in* PRIVACY IMPACT ASSESSMENT 385, 395 (David Wright & Paul De Hert eds., 2012).

211. For a critical perspective on privacy nudges see Willis, *supra* note 144, at 1170-72. "Nudges may not be an effective way to help people make better choices about information privacy; accordingly, firms can use the same mechanisms and conditions that make nudges work to make nudges fail." *Id.*

212. *Final Report of the European Union Privacy Seals Project on the Inventory and*

Finally, behavioural insights could be introduced to evaluate ex post the goodness of a law (or piece of law) to improve people's privacy life: learn from the experience (how people reacted to a specific public intervention in the privacy field) and take the consequent policy decisions.

Having said that, a word of caution is required. While it would be naïve to ignore the effect of biases when setting a privacy policy that relies on the decisions of people, we should, however, not totally rely on the effects of biases. First, privacy choices are context-dependent. Therefore, EU future strategies should consider and possibly guide the choice of what privacy nudge is better for a specific context (e.g., informal, youngish context).

Secondly, as recent behavioural research in the law domain also teach us, implementing nudging mechanisms might not be enough to protect online privacy, especially in contexts such as behavioural targeting by companies: we cannot easily rely on user's behaviour change when personal data disclosure is the only way to obtaining a service: in cases such as news programing or webpages targeting kids,[213] prohibitions and a duly control system of certain companies practices are needed.[214] Recent studies have shown that many companies might not obey what they promise in their privacy policies or that they do not respect the users' preference, for instance, not to receive unsolicited commercial emails. [215] Therefore, there will be always some aspects that needs coercive regulatory tools.

In other words, privacy visceral notices might not be considered as a panacea to protect privacy, but complementary tools. Sometimes, coercive measures are still necessary: (1) when personal data is necessary to obtain a public service; (2) in general, technical processes and mechanisms specific of big data[216] make users unaware of what decisions

---

Analysis of Certification Schemes, at 12 (2013), *available at* http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf (last visited Dec. 20, 2015).

213. *See* Simone van der Hof, *No Child's Play: Online Data Protection for Our Children*, *in* MINDING MINORS WANDERING THE WEB: REGULATING ONLINE CHILD SAFETY 127, 130 (Simone van der Hof et al. eds., 2014).

214. Borgesius, *supra* note 80, at 5, 46.

215. Some tests with unsolicited commercial emails ("UCE") show that only one out of three websites respect the will of the data subject not to receive commercial communications. *See* Maurizio Borghi et al., *Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence From The UK*, 21 INT'L J.L. & INFO. TECH. 109, 152 (2013) (reporting that their study, conducted on popular UK-based websites, "unveils that the way in which websites obtain consent (opt-in, pre-selected opt-in, or opt-out) is not a proxy of lawful processing of data at a later stage").

216. Cukier & Mayer-Schoenberger, *supra* note 81, at 6.

will be taken on the basis of their data; and (3) online companies might not be compliant with their policies. Even if they advertise their website as privacy-protective, thus increasing users' trust, their promises to respect users' privacy preferences might be infringed, without users being able to realize it. Privacy seals might prove to be an instrument for competition among companies that, however, centers on privacy image rather than privacy reality.[217] Moreover, online companies may use the same mechanisms that make nudges work to make nudges fail, like reframing the nudges: "a push [back] can easily overwhelm a nudge."[218]

Therefore, in order to make sure that tested privacy nudges work as expected also in real life, public policy should learn the lessons of behavioural science, being capable to guide and check not only the creation (design) but also the use of these nudges; it may be necessary to impose requirements and conditions, not only on the appearance of a privacy nudge, but on the effects it pursues. Also, for privacy seals to work and given the difficulty for users to distinguish websites on privacy grounds, it would be necessary to increase the driving and supervisory powers of data protection authorities, which can verify the *truthfulness* of privacy seals (or other certification model) and strengthen their effect.

1. *Future research*

Online companies may be non-compliant with data protection law for different reasons, including the lack of appropriate standard of information on what the law requires, as well as a lack adequate supervision mechanisms.[219] On this regard, future research may explore possibilities for nudging systems to target the companies themselves, i.e., to drive them to be compliant with data protection law.

For future research, cyber-security risks (besides and in addition to those for privacy and data protection) should also be considered. Accidental or intentional personal data breaches (e.g., as consequence of, but not limited to, hacking activity), as well as identity thefts (perpetrated, for instance to commit financial crimes) are still far from being defeated. However, the security in cyberspace may be benefited and improved

217. Lauren E. Willis, *Why Not Privacy by Default?*, 29 BERKELEY TECH. L.J. 64, 128 (2014).

218. *Id.* at 131.

219. Borghi et al., *supra* note 215, at 110, 153 (claiming that there is a severe lack of compliance of UK online service providers with essential requirements of data protection law and suggest that this might due to the existence of "an inappropriate standard of implementation, information and supervision by the UK authorities, rather than of a conscious infringing behavior." As they notice, "unclear or unexplained law is detrimental to the development of a safe online environment and, ultimately, to citizens").

precisely through nudging systems,[220] including the use of privacy and security nudges. These might take the form of visceral notices, as described in this text, or of other kinds of nudging mechanisms.[221] Further research should also investigate *the long-term* impact of visceral notices and privacy nudges in general and observe users' privacy behaviours over time.[222]

V. CONCLUSIVE REMARKS

The behaviourally-informed approach to regulatory problems, in fact, is gaining momentum, and its instruments, so called *nudges*, are becoming authentic policy tools. To what extent behavioural insights can be applied to policy-making in the field of *privacy* and how? Building upon few existing experiments on users' attitudes and behaviour as regards privacy, this paper aims at bringing behavioural research methods for *privacy* to the attention of policymakers, exploring challenges and opportunities of applying behavioural insights into privacy policy-making, at its different stages: from the design to the implementation phase.

After having discussed the reasons of the failure of traditional information notices (privacy policies) and considered the benefits of applying behavioural insights for regulatory purposes in general (e.g., *nudging* strategies), this article claims that the introduction of *privacy nudges*, as complementary regulatory tools can be considered legitimate and worthy of policy support, also in Europe, as far as: (1) they seek at encouraging a privacy-enhancing behaviour, while preserving the freedom of choice of the users (rather than hinder it), as soft or libertarian paternalism claims;[223] and (2) they are adopted in a transparent manner and subject to oversight mechanisms to guarantee that base legal principles are respected.

Also, the paper aims to trigger the discussion on the feasibility of introducing specific legal requirements for effective privacy notices (whether on a privacy-by-design architecture or also on the purposes to be pursued, i.e., the behavioural change).

After all, the new Proposal for a European GDPR,[224] seeks to reinforce the transparency and informed consent requirements in view of

220. *See Work Packages*, SPION (Dec. 21, 2012), *available at* http://www.spion.me/workpackages/ (last visited Dec. 20, 2015).

221. van der Berg, *supra* note 108, at 776, 783.

222. Groom & Calo, *supra* note 25, at 4, 28.

223. THALER & SUNSTEIN, *supra* note 131, at 5.

224. *See Proposal for GDPR*, *supra* note 2.

strengthening individual rights. Behavioural insights and nudging systems (as *visceral notices*) may represent an evolving way of interpreting and implementing the new Regulation, or a way of testing the adequacy of its stated safeguards.